



Index formulae for Stark units and their solutions

Xavier-François Roblot

► To cite this version:

Xavier-François Roblot. Index formulae for Stark units and their solutions. Pacific Journal of Mathematics, 2013, 266 (2), pp.391-422. hal-00863158

HAL Id: hal-00863158

<https://hal.science/hal-00863158>

Submitted on 19 Sep 2013

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

INDEX FORMULAE FOR STARK UNITS AND THEIR SOLUTIONS

XAVIER-FRANÇOIS ROBLOT

ABSTRACT. Let K/k be an abelian extension of number fields with a distinguished place of k that splits totally in K . In that situation, the abelian rank one Stark conjecture predicts the existence of a unit in K , called the Stark unit, constructed from the values of the L -functions attached to the extension. In this paper, assuming the Stark unit exists, we prove index formulae for it. In a second part, we study the solutions of the index formulae and prove that they admit solutions unconditionally for quadratic, quartic and sextic (with some additional conditions) cyclic extensions. As a result we deduce a weak version of the conjecture (“up to absolute values”) in these cases and precise results on when the Stark unit, if it exists, is a square.

1. INTRODUCTION

Let K/k be an abelian extension of number fields. Denote by G its Galois group. Let S_∞ and S_{ram} denote respectively the set of infinite places of k and the set of finite places of k ramified in K/k . Let $S(K/k) := S_\infty \cup S_{\text{ram}}$. Fix a finite set S of places of k containing $S(K/k)$ and of cardinality at least 2. Assume that there exists at least one place in S , say v , that splits totally in K/k and fix a place w of K dividing v . Let e be the order of the group of roots of unity in K . In this setting Stark [14] made the following conjecture.

Conjecture (ABELIAN RANK ONE STARK CONJECTURE).

There exists an S -unit $\varepsilon_{K/k,S}$ in K such that

- (1) *For all characters χ of G*

$$L'_{K/k,S}(0, \chi) = \frac{1}{e} \sum_{g \in G} \chi(g) \log |\varepsilon_{K/k,S}^g|_w$$

where $L_{K/k,S}(s, \chi)$ denotes the L -function associated to χ with Euler factors at prime ideals in S deleted.

- (2) *The extension $K(\varepsilon_{K/k,S}^{1/e})/k$ is abelian.*
 (3) *If furthermore $|S| \geq 3$ then ε is a unit of K .*

The unit $\varepsilon_{K/k,S}$ is called the Stark unit associated to the extension K/k , the set of places S and the place v .¹ It is unique up to multiplication by a root of unity in K . A good reference for this conjecture is [15, Chap. IV].

The starting point of this research is the conjectural method used in [3] and [10] (and inspired by [13]) to construct totally real abelian extensions of totally real fields. Let L/k be such an extension. The idea is to construct a quadratic extension K/L , abelian over k , satisfying some additional conditions similar to the assumptions (A1), (A2) and

Date: July 11, 2013.

Supported by the JSPS Global COE *CompView*. This research was conducted while the author was a member of the Department of Mathematics of the Tokyo Institute of Technology, 2-12-1 Ookayama, Meguro-ku, Tokyo 152-8550, Japan .

¹In fact the place w but changing the place w just amounts to replace the Stark unit by one of its conjugate.

(A3) below. Assuming the Stark conjecture for K/k , $S(K/k)$ and a fixed real place v of k , one can prove that $K = k(\varepsilon)$ and $L = k(\alpha)$ where $\alpha := \varepsilon + \varepsilon^{-1}$ and $\varepsilon := \varepsilon_{K/k, S(K/k)}$ is the corresponding Stark unit. Using part (1) of the conjecture, one computes the minimal polynomial $A(X)$ of α over k . The final step is to check unconditionally that the polynomial $A(X)$ does indeed define the extension L .

One notices in that setting that the rank of the units of K is equal to the rank of units of L plus the rank of the module generated by the Stark unit and its conjugates over k . A natural question to ask is whether the index of the group generated by the units of L and the conjugates of the Stark unit has finite index inside the group of units of K and, if so, if this index can be computed. A positive answer to the first question is given by Stark in [12, Th. 1]. In [1], Arakawa gives a formula for this index when k is a quadratic field. Using similar methods, we obtain a general result (Theorem 2.2) in the next section. Then we derive a “relative” index formula (Theorem 2.3) that relates the index of the subgroup generated over $\mathbb{Z}[G]$ by the Stark unit inside the “minus-part” of the group of units of K to the cardinality of the “minus-part” of the class group of K .² In the third section, we use results of Rubin [11] on a form of the Gras conjecture for Stark units to show that the relative index formula implies local relative index formulae (Theorem 3.2). Starting with the fourth section, we stop assuming the abelian rank one Stark conjecture and study directly the solutions to the index formulae. In section 4, we look at how much these index formulae characterize the Stark unit (Proposition 4.1 and Corollary 4.5). In the next section, we introduce the algebraic tools that will be needed to prove the existence of solutions in some cases in the following sections. We also reprove in that section the abelian rank one Stark conjecture for quadratic extensions (Theorem 5.5). Finally, sections 6 and 7 are devoted to a proof that solutions to the index formulae always exist for quartic extensions (Theorem 6.1) and sextic extensions (Theorem 7.1) with some additional conditions in that case. We show that the existence of solutions in those cases imply a weak version of the conjecture where part (1) is satisfied only up to absolute values.³ We also obtain results on when the Stark unit, if it exists, is a square (Corollary 2.4, Theorem 5.5, Corollary 6.2 and Corollary 7.2).

2. THE INDEX FORMULAE

We assume from now on that the place v is infinite⁴ and that k has at least two infinite places. Therefore we can always apply the conjecture for any finite set S containing $S(K/k)$. The cases that we are excluding are $k = \mathbb{Q}$ and k a complex quadratic field. In both cases the conjecture is proved and the Stark unit is strongly related to cyclotomic units and elliptic units respectively.

Fix a finite set S of places of k containing $S(K/k)$. We make the following additional assumptions.

- (A1) k is totally real and the infinite places of K above v are real, the infinite places of K not above v are complex.
- (A2) The maximal totally real subfield K^+ of K satisfies $[K : K^+] = 2$.
- (A3) All the finite primes in S are either ramified or inert in K/K^+ .

²Similar in some way to the index formulae for cyclotomic units, see [17, Chap. 8].

³Unfortunately, in most cases the values are complex and there does not appear to be any obvious way to remove these absolute values.

⁴For v a finite place, the abelian rank one Stark conjecture is basically equivalent to the Brumer-Stark conjecture, see [15, §IV.6]. Recent results of Greither and Popescu [5] imply the validity of the Brumer-Stark conjecture away from its 2-part and under the hypothesis that an appropriate Iwasawa μ -invariant vanishes.

If S contains more than one place that splits totally in K/k then the conjecture is trivially true with the Stark unit being equal to 1. Therefore the only non trivial case excluded by (A1) is the case when k has exactly one complex place and K is totally complex. It is likely that most of the methods and results in this paper can be adapted to cover also that case. Assumptions (A2) and (A3) are necessary to ensure that the rank of the group generated by the units of K^+ and the conjugate of the Stark unit has finite index inside the group of units of K . Without these assumptions, global index formulae for Stark units as they are stated in this article cannot exist although it is still possible to prove index formulae for some p -adic characters if one takes also into account Stark units coming from subextensions (see [11] or Section 3).

We assume until further notice that the conjecture is true for the extension K/k , the set of places S and the distinguished place v .⁵

Denote by $\varepsilon := \varepsilon_{K/k,S}$ the corresponding Stark unit. From now on, all subfields of K (including K itself) are identified with their image in \mathbb{R} by w . We make the Stark unit unique by imposing that $\varepsilon > 0$. It follows that $\varepsilon^g > 0$ for all $g \in G$, see [15, §IV.3.7]. One can also prove under these hypothesis, see [10, Lem. 2.8], that $|S(K/k)| \geq 3$ and therefore ε is a unit of K by part (3) of the Conjecture, and that $|\varepsilon|_{w'} = 1$ for any place w' of K not above v .

Let m be the degree of K^+/k and d be the degree of k/\mathbb{Q} . Thus we have $[K : k] = 2m$ and $[K : \mathbb{Q}] = 2md$. Let τ denote the non trivial element of $\text{Gal}(K/K^+)$. It is the complex conjugation of the extension K and, by the above remark, we have $\varepsilon^\tau = \varepsilon^{-1}$. Let G^+ denote the Galois group of K^+/k , thus $G^+ \cong G/\langle \tau \rangle$. It follows from (A1) that the signatures of K^+ and K are respectively $(dm, 0)$ and $(2m, m(d-1))$. Therefore the rank of U_{K^+} and U_K , the group of units of K^+ and K , are respectively $dm - 1$ and $2m + m(d-1) - 1 = (dm - 1) + m$. Let U_{Stark} be the multiplicative $\mathbb{Z}[G]$ -module generated by ± 1 , ε and U_{K^+} . Let $R := \{\rho_1, \dots, \rho_m\}$ be a fixed set of representatives of G modulo $\langle \tau \rangle$. Set $\varepsilon_\ell := \rho_\ell^{-1}(\varepsilon)$ for $\ell = 1, \dots, m$. Since $\tau(\varepsilon) = \varepsilon^{-1}$, the group U_{Stark} is generated over \mathbb{Z} by $\{\pm 1, \eta_1, \dots, \eta_{dm-1}, \varepsilon_1, \dots, \varepsilon_m\}$ where $\eta_1, \dots, \eta_{dm-1}$ is a system of fundamental units of K^+ . Let $|\cdot|_j$, $1 \leq j \leq (d+1)m$ denote the infinite normalized absolute values of K ordered in the following way. The $2m$ real absolute values of K , corresponding to the places over v , are $|\cdot|_j := |\rho_j(\cdot)|$ and $|\cdot|_{j+m} := |\rho_j\tau(\cdot)|$ for $1 \leq j \leq m$. The complex absolute values, corresponding to the infinite places not above v , are $|\cdot|_j$ for $2m+1 \leq j \leq (d+1)m$. The regulator of U_{Stark} is the absolute value of the determinant of the following matrix⁶

$$\left(\log |\eta_i|_j \mid \log |\varepsilon_\ell|_j \right)_{j,(i,\ell)}$$

where $1 \leq j \leq (d+1)m - 1$, $1 \leq i \leq dm - 1$ and $1 \leq \ell \leq m$. For $1 \leq j \leq (d+1)m$, let $|\cdot|_j^+$ denote the restriction of the absolute value $|\cdot|_j$ to K^+ . For $1 \leq j \leq m$, the places corresponding to $|\cdot|_j$ and $|\cdot|_j^+$ are real and $\log |\eta_i|_j^+ = \log |\eta_i|_j = \log |\eta_i|_{j+m}$. For $2m+1 \leq j \leq (d+1)m$, the places corresponding to $|\cdot|_j$ and $|\cdot|_j^+$ are respectively complex and real, thus $\log |\eta_i|_j^+ = 2 \log |\eta_i|_j$. Note also that $|\varepsilon_\ell|_{j+m} = |\varepsilon_\ell|_j^{-1}$ for $1 \leq j \leq m$ and $|\varepsilon_\ell|_j = 1$ for $2m+1 \leq j \leq (d+1)m$. Therefore the matrix is equal to

$$\left(\begin{array}{c|c} \log |\eta_i|_j^+ & \log |\varepsilon_\ell|_j \\ \hline \log |\eta_i|_j^+ & -\log |\varepsilon_\ell|_j \\ \hline 2 \log |\eta_i|_{j'}^+ & 0 \end{array} \right)_{(j,j'),(i,\ell)}$$

⁵Since v is the only real place of k that stays real in K , we will usually not specify it.

⁶We discard the last absolute value $|\cdot|_{(d+1)m}$.

where $1 \leq j \leq m$, $2m+1 \leq j' \leq (d+1)m-1$, $1 \leq i \leq dm-1$ and $1 \leq \ell \leq m$. Now we add the j -th row to the $(m+j)$ -th row for $1 \leq j \leq m$ and we obtain finally the following matrix with the same determinant

$$\left(\begin{array}{c|c} \log |\eta_i|_j^+ & \log |\varepsilon_\ell|_j \\ \hline 2 \log |\eta_i|_j^+ & 0 \\ \hline 2 \log |\eta_i|_{j'}^+ & 0 \end{array} \right)_{(j,j'),(i,\ell)}.$$

Therefore the regulator of U_{Stark} is

$$\text{Reg}(U_{\text{Stark}}) = \left| \det(\log |\varepsilon_\ell|_j)_{j,\ell} \det \left(2 \log |\eta_i|_{j'}^+ \right)_{j',i} \right| \quad (2.1)$$

where $1 \leq \ell, j \leq m$, $1 \leq i \leq dm-1$ and j' runs through the set $\{1, \dots, m, 2m+1, \dots, (d+1)m-1\}$. The absolute values $|\cdot|_1^+, \dots, |\cdot|_m^+, |\cdot|_{2m+1}^+, \dots, |\cdot|_{(d+1)m-1}^+$ are the absolute values corresponding to all the infinite places of K^+ but one. Thus the second term is $2^{dm-1} R_{K^+}$. For the first term, we have

$$|\det(\log |\varepsilon_\ell|_j)_{j,\ell}| = |\det(\log |\varepsilon^{\rho\lambda^{-1}}|)_{\rho,\lambda \in R}|.$$

We say that a character χ of G is even if $\chi(\tau) = 1$, otherwise χ is odd and $\chi(\tau) = -1$. The even characters of G are the inflations of characters of G^+ . We have the following modification of the classical determinant group factorization.

Lemma 2.1. *Let $a_g \in \mathbb{C}$, for $g \in G$, be such that $a_{\tau g} = -a_g$ for all $g \in G$. Then*

$$\det(a_{\rho\lambda^{-1}})_{\rho,\lambda \in R} = \prod_{\chi \text{ odd}} \sum_{\rho \in R} \chi(\rho) a_\rho.$$

Proof. Let E be the \mathbb{C} -vector space of functions $f : G \rightarrow \mathbb{C}$ such that $f(\tau g) = -f(g)$ for all $g \in G$. Clearly it has dimension m and admits $(\chi)_{\chi \text{ odd}}$ has a basis. Another basis is given by the functions $(\delta_\rho)_{\rho \in R}$ defined by

$$\delta_\rho(\rho) = 1, \delta_\rho(\tau\rho) = -1 \text{ and } \delta_\rho(g) = 0 \text{ for all } g \in G \text{ with } g \neq \rho, \tau\rho.$$

The group G acts on E by $f^\sigma : g \mapsto f(g\sigma)$ for $f \in E$ and $\sigma \in G$. In particular, we have $f^\tau = -f$. We extend this action linearly to give E a structure of $\mathbb{C}[G]$ -module. Now consider the endomorphism defined by $T := \sum_{g \in G} a_g g$. We have

$$T(\delta_\rho) = \sum_{\substack{g \in G \\ \rho g^{-1} \in R}} a_g \delta_\rho^g + \sum_{\substack{g \in G \\ \rho g^{-1} \notin R}} a_g \delta_\rho^g = \sum_{\substack{g \in G \\ \rho g^{-1} \in R}} a_g \delta_{\rho g^{-1}} - \sum_{\substack{g \in G \\ \rho g^{-1} \notin R}} a_g \delta_{\tau \rho g^{-1}}.$$

We write $\lambda = \rho g^{-1}$ in the first sum and $\lambda = \tau \rho g^{-1}$ in the second one. We get

$$T(\delta_\rho) = \sum_{\lambda \in R} a_{\rho\lambda^{-1}} \delta_\lambda - \sum_{\lambda \in R} a_{\tau\rho\lambda^{-1}} \delta_\lambda = 2 \sum_{\lambda \in R} a_{\rho\lambda^{-1}} \delta_\lambda.$$

Therefore the determinant of T is $2^m \det(a_{\rho\lambda^{-1}})_{\rho,\lambda \in R}$. On the other hand, for χ odd, we compute

$$T(\chi) = \sum_{g \in G} a_g \chi^g = \sum_{g \in G} a_g \chi(g) \chi.$$

Thus χ is an eigenvector for T with eigenvalue $\sum_{g \in G} a_g \chi(g) = 2 \sum_{\rho \in R} \chi(\rho) a_\rho$. Therefore

$\det(T) = 2^m \prod_{\chi \text{ odd}} \sum_{\rho \in R} \chi(\rho) a_\rho$ and the result follows. \square

By the lemma, we get

$$\begin{aligned} \det(\log |\varepsilon^{\rho\lambda^{-1}}|)_{\rho, \lambda \in R} &= \prod_{\chi \text{ odd}} \sum_{\rho \in R} \chi(\rho) \log |\varepsilon^\rho| = \prod_{\chi \text{ odd}} \frac{1}{2} \sum_{g \in G} \chi(g) \log |\varepsilon^g| \\ &= \prod_{\chi \text{ odd}} L'_{K/k, S}(0, \chi) \end{aligned} \quad (2.2)$$

using part (1) for the last equality and the fact that the number of roots of unity in K is 2 since K is not totally complex by (A1). On the other hand, we have

$$\prod_{\chi \text{ odd}} L_{K/k, S}(s, \chi) = \frac{\zeta_{S, K}(s)}{\zeta_{S, K^+}(s)} \quad (2.3)$$

where $\zeta_{S, K}(s) := \zeta_{S_K, K}(s)$ and $\zeta_{S, K^+}(s) := \zeta_{S_{K^+}, K^+}(s)$ denote respectively the Dedekind zeta functions of K and K^+ with the Euler factors at primes in S_K and S_{K^+} removed. Here S_K and S_{K^+} denote respectively the set of places of K and of K^+ above the places in S . We will often use by abuse the subscript S instead of S_K or S_{K^+} to simplify the notation. Taking the limit when $s \rightarrow 0$ in (2.3) and using the expression for the Taylor development at $s = 0$ of Dedekind zeta functions, see [15, Cor. I.1.2], we get

$$\prod_{\chi \text{ odd}} L'_{K/k, S}(0, \chi) = 2^{t_S} \frac{h_K R_K}{h_{K^+}^+ R_{K^+}^+} \quad (2.4)$$

where t_S is the number of prime ideals in S_{K^+} that are inert in K/K^+ and h_K , R_K , h_{K^+} and R_{K^+} are respectively the class numbers and regulators of K and K^+ . Putting together equations (2.1), (2.2) and (2.4), we get the following result.

Theorem 2.2. *The index of U_{Stark} in the group of units of K is*

$$(U_K : U_{\text{Stark}}) = 2^{t_S + dm - 1} \frac{h_K}{h_{K^+}}$$

where t_S is the number of prime ideals in S_{K^+} that are inert in K/K^+ . \square

Let Cl_K and Cl_{K^+} denote respectively the class groups of K and K^+ . Define Cl_K^- and U_K^- as the kernel of the following maps induced by the norm $\mathcal{N} := 1 + \tau$ of the extension K/K^+

$$\text{Cl}_K^- := \text{Ker}(\mathcal{N} : \text{Cl}_K \rightarrow \text{Cl}_{K^+}) \quad \text{and} \quad U_K^- := \text{Ker}(\mathcal{N} : \bar{U}_K \rightarrow \bar{U}_{K^+})$$

where \bar{U}_K and \bar{U}_{K^+} are respectively $U_K/\{\pm 1\}$ and $U_{K^+}/\{\pm 1\}$. From now on, we use the additive notation to denote the action of $\mathbb{Z}[G]$, and other group rings, on \bar{U}_K and its subgroups $U_K^-, \bar{U}_{K^+}, \dots$. For $x \in U_K$, we denote by \bar{x} its class in \bar{U}_K and adopt the following convention: if $\bar{x} \in \bar{U}_K$, we let x denote the unique element in the class \bar{x} such that $x > 0$. Note that $\mathcal{N}(x) = \mathcal{N}(-x) = 1$ since K/K^+ is ramified at at least one real place.

Theorem 2.3. *We have*

$$(U_K^- : \mathbb{Z}[G] \cdot \bar{\varepsilon}) = 2^{e+t_S} |\text{Cl}_K^-|$$

where $2^e = (\bar{U}_{K^+} : \mathcal{N}(\bar{U}_K))$.

Proof. By class field theory the map $\mathcal{N} : \text{Cl}_K \rightarrow \text{Cl}_{K^+}$ is surjective. Therefore $|\text{Cl}_K^-| = h_K/h_{K^+}$. On the other hand, if we let $\bar{U}_{\text{Stark}} := U_{\text{Stark}}/\{\pm 1\}$, we have

$$\text{Ker}(\mathcal{N} : \bar{U}_{\text{Stark}} \rightarrow \bar{U}_{K^+}) = \mathbb{Z}[G] \cdot \bar{\varepsilon} \quad \text{and} \quad \text{Im}(\mathcal{N} : \bar{U}_{\text{Stark}} \rightarrow \bar{U}_{K^+}) = 2 \cdot \bar{U}_{K^+}.$$

Therefore we get

$$(\bar{U}_K : \bar{U}_{\text{Stark}}) = (\mathcal{N}(\bar{U}_K) : 2 \cdot \bar{U}_{K^+}) (U_K^- : \mathbb{Z}[G] \cdot \bar{\varepsilon}).$$

Since $(\bar{U}_K : \bar{U}_{\text{Stark}}) = (U_K : U_{\text{Stark}})$, it follows from Theorem 2.2 that

$$(U_K^- : \mathbb{Z}[G] \cdot \bar{\varepsilon}) = \frac{2^{t_S + dm - 1} |\text{Cl}_K^-|}{(\mathcal{N}(\bar{U}_K) : 2 \cdot \bar{U}_{K+})}.$$

We conclude by noting that

$$(\mathcal{N}(\bar{U}_K) : 2 \cdot \bar{U}_{K+}) = \frac{(\bar{U}_{K+} : 2 \cdot \bar{U}_{K+})}{(\bar{U}_{K+} : \mathcal{N}(\bar{U}_K))} = \frac{2^{dm-1}}{(\bar{U}_{K+} : \mathcal{N}(\bar{U}_K))}. \quad \square$$

It has been observed that the Stark unit is quite often a square. The theorem provides us with a necessary condition for that to happen.

Corollary 2.4. *Let c be the 2-valuation of the order of Cl_K^- . A necessary condition for the Stark unit ε to be a square in K is*

$$e + t_S + c \geq m.$$

Proof. Assume that $\varepsilon = \eta^2$ with $\eta \in K$. Then it is easy to see that $\eta \in U_K^-$ and therefore $(\mathbb{Z}[G] \cdot \bar{\eta} : \mathbb{Z}[G] \cdot \bar{\varepsilon}) = 2^m$ divides $2^{e+t_S} |\text{Cl}_K^-|$. \square

We will see below, see (5.10), that $e \geq (d-1)m - 2$. Therefore the inequality in the theorem is always satisfied for $d \geq 2 + 2/m$. However, this is not enough to ensure that the Stark unit is a square in general. Indeed at the end of the paper we give an example of a cyclic sextic extension K/k satisfying (A1), (A2) and (A3), and with k a totally real cubic field where the Stark unit, assuming it exists, is not a square even though $e > m$. But, in all the cases that we study, we can prove that for d sufficiently large the Stark unit is always a square. Of course these cases are quite specific and it is difficult to draw from them general conclusions, but still we are lead to ask the following question.

Question. Fix a relative degree m . Does there exist a constant $D(m)$, depending only on m , such that for any extensions K/k of degree $2m$ and any finite set of places S containing $S(K/k)$ satisfying (A1), (A2) and (A3), and with $d \geq D(m)$, the corresponding Stark unit, assuming that it exists, is always a square in K ?

It follows from the result of the next sections that the answer is positive for $1 \leq m \leq 3$ and that $D(1) = D(3) = 4$ and $D(2) = 3$.

3. RUBIN'S INDEX FORMULA

In [11], Rubin proves Gras conjecture type results for Stark units using Euler systems. His results are generalized by Popescu [9]. In this section, we use the results of Rubin to get a similar result in our setting. To be able to use Rubin's results we need to make the following additional assumption:

(A4) K contains the Hilbert Class Field H_k of k .

We assume in this section that the conjecture is true for the extensions and set of places as described in [11].

We first introduce the results of Rubin. Let \mathfrak{f} be the conductor of K/k . For any modulus \mathfrak{g} dividing \mathfrak{f} , let $K_{\mathfrak{g}} = K \cap k(\mathfrak{g})$ be the intersection of K with the ray class field of k of conductor \mathfrak{g} . Since v is totally split in K/k , one can apply the conjecture to the extension $K_{\mathfrak{g}}/k$, the set of places $S(K_{\mathfrak{g}}/k)$ and the place v , and get a Stark unit that we denote by $\varepsilon_{\mathfrak{g}}$. Let $G_{\mathfrak{g}}$ be the Galois group of $K_{\mathfrak{g}}/k$. Note that by (A1) the group of roots of unity in $K_{\mathfrak{g}}$ is $\{\pm 1\}$. Part (2) of the conjecture is equivalent to the fact that $\varepsilon_{\mathfrak{g}}^{g-1} \in U_{K_{\mathfrak{g}}}^2$ for all $g \in G_{\mathfrak{g}}$, see [15, Prop. IV.1.2]. Define R_{Stark} as the following $\mathbb{Z}[G]$ -module

$$R_{\text{Stark}} = \langle \pm 1, (\varepsilon_{\mathfrak{g}}^{g-1})^{1/2} \text{ for } \mathfrak{g} \mid \mathfrak{f} \text{ and } g \in G_{\mathfrak{g}} \rangle_{\mathbb{Z}[G]}.$$

Let p be a prime number that does not divide the order of G . In particular, p is an odd prime. Denote by \hat{G}_p the set of irreducible \mathbb{Z}_p -characters of G . For $\psi \in \hat{G}_p$ and M a $\mathbb{Z}[G]$ -module, we set

$$M^\psi := M \otimes_{\mathbb{Z}[G]} \mathbb{Z}_p[\psi]$$

where $\mathbb{Z}_p[\psi]$ is the ring generated over \mathbb{Z}_p by the values of ψ and G acts on $\mathbb{Z}_p[\psi]$ via the character ψ . The following result is a direct consequence of Theorem 4.6 of [11].

Theorem 3.1 (RUBIN). *If $\psi \in \hat{G}_p$ is odd then*

$$\left| (U_K/R_{\text{Stark}})^\psi \right| = \left| \text{Cl}_K^\psi \right|.$$

From this we deduce an analogous statement for our case.

Theorem 3.2. *For all $\psi \in \hat{G}_p$, we have*

$$\left| (U_K^-/\mathbb{Z}[G] \cdot \bar{\varepsilon})^\psi \right| = \left| (\text{Cl}_K^-)^\psi \right|.$$

Proof. For M a $\mathbb{Z}[G]$ -module and $\psi \in \hat{G}_p$, it is direct to see that $M^\psi = (M^{1+\tau})^\psi$ if ψ is even and $M^\psi = (M^{1-\tau})^\psi$ if ψ is odd. In particular, if ψ is even, we get $|(U_K^-/\mathbb{Z}[G] \cdot \bar{\varepsilon})^\psi| = |(\text{Cl}_K^-)^\psi| = 1$ and the result follows trivially in that case. Assume now that ψ is odd. Let ε_0 be the Stark unit corresponding to the extension K/k , the set of places $S(K/k)$ and the distinguished place v . Assume first that $S = S(K/k) \cup \{\mathfrak{p}\}$ for some finite prime ideal \mathfrak{p} of k not in $S(K/k)$. It follows from [15, Prop. IV.3.4] that $\bar{\varepsilon} = (1 - F_{\mathfrak{p}}(K/k)) \cdot \bar{\varepsilon}_0$ where $F_{\mathfrak{p}}(K/k)$ is the Frobenius at \mathfrak{p} for the extension K/k . By (A3), τ is a power of $F_{\mathfrak{p}}(K/k)$ and thus $\psi(F_{\mathfrak{p}}(K/k))$ is a non trivial root of unity of order dividing $|G|$. Then $1 - \psi(F_{\mathfrak{p}}(K/k))$ is a p -adic unit and therefore $(\mathbb{Z}[G] \cdot \bar{\varepsilon})^\psi = (\mathbb{Z}[G] \cdot \bar{\varepsilon}_0)^\psi$. By repeating this argument if necessary, we see that this last equality also holds in the general case. Now, by taking $\mathfrak{g} = \mathfrak{f}$ and $\sigma = \tau$ in the definition of R_{Stark} , we see that $\varepsilon_0^{(\tau-1)/2} = \varepsilon_0^{-1} \in R_{\text{Stark}}$. Therefore we have $\varepsilon_0^{\mathbb{Z}[G]} \subset R_{\text{Stark}} \subset U_K$, and thus

$$\varepsilon_0^{2\mathbb{Z}[G]} \subset R_{\text{Stark}}^{\tau-1} \subset U_K^{\tau-1}.$$

We take the ψ -component, by the above remarks and the theorem, we get

$$\begin{aligned} |(U_K^-/\mathbb{Z}[G] \cdot \bar{\varepsilon})^\psi| &= |(U_K^-/\mathbb{Z}[G] \cdot \bar{\varepsilon}_0)^\psi| = |(U_K^{\tau-1}/\varepsilon_0^{2\mathbb{Z}[G]})^\psi| \geq \\ &= |(U_K^{\tau-1}/R_{\text{Stark}}^{\tau-1})^\psi| = |(U_K/R_{\text{Stark}})^\psi| = |\text{Cl}_K^\psi| = |(\text{Cl}_K^-)^\psi|. \end{aligned}$$

Assume there exists a character ψ for which this is a strict inequality. Multiplying over all characters in \hat{G}_p , we get $|(U_K^-/\mathbb{Z}[G] \cdot \bar{\varepsilon}) \otimes \mathbb{Z}_p| > |\text{Cl}_K^- \otimes \mathbb{Z}_p|$, a contradiction with Theorem 2.3. Therefore the equality holds for all $\psi \in \hat{G}_p$ and the theorem is proved. \square

4. THE INDEX PROPERTY

From now on, we do not assume any more that the conjecture is true.

From the results of the previous sections, we see that the conjecture implies that there exists a unit $\bar{\varepsilon} \in U_K^-$ such that⁷

- (P1) $(U_K^- : \mathbb{Z}[G] \cdot \bar{\varepsilon}) = 2^{e+ts} |\text{Cl}_K^-|$,
- (P2) $|(U_K^-/\mathbb{Z}[G] \cdot \bar{\varepsilon})^\psi| = |(\text{Cl}_K^-)^\psi|$ for all $p \nmid [K : k]$ and $\psi \in \hat{G}_p$.

⁷Although assumptions (A1) to (A4) are necessary to prove that the Stark unit is a solution of (P2), it is not necessary to assume (A4) to prove that solutions exist in the cases that we study below. It is an interesting question whether or not one could prove that the Stark unit is a solution to (P2) without having first to assume (A4).

A priori the existence of a solution to (P1) and (P2) does not imply in return the conjecture (except for quadratic extensions, see Theorem 5.5 below). Indeed, in general, properties (P1) and (P2) do not even characterize the Stark unit ε . To see that assume that $\bar{\eta}$ is a solution to (P1) and (P2), and let $\bar{\eta}' := u \cdot \bar{\eta}$ where $u \in \mathbb{Z}[G]^\times$ is a unit of $\mathbb{Z}[G]$. Then $\bar{\eta}'$ also satisfies (P1) and (P2). If u belongs to $\{\pm\gamma : \gamma \in G\} \subset \mathbb{Z}[G]^\times$, the group of trivial units of $\mathbb{Z}[G]$, then $\bar{\eta}'$ is essentially the *same solution* since it is a conjugate of $\bar{\eta}$ or the inverse of a conjugate of $\bar{\eta}$. However there may be some non trivial units in $\mathbb{Z}[G]$ (see the end of this section) and thus solutions to (P1) and (P2) that are not related in any obvious way to the Stark unit. In any case, we have the following result that shows that solutions to (P1) satisfy a very weak version of part (1) of the conjecture.

Proposition 4.1. *Let $\bar{\eta}$ be an element of U_K^- satisfying (P1). Then we have*

$$\prod_{\chi \text{ odd}} \frac{1}{2} \sum_{g \in G} \chi(g) \log |\eta^g| = \pm \prod_{\chi \text{ odd}} L'_{K/k,S}(0, \chi). \quad (4.5)$$

Proof. Let $\bar{x} \in U_K^-$. Using the notations of Section 2, we have $|x^\tau|_j = |x|_j$ for $2m+1 \leq j \leq (d+1)m$ since these absolute values are complex and τ is the complex conjugation. Since, by construction, we have $x^\tau = x^{-1}$, it follows that $|x|_j^2 = |x^{1+\tau}|_j = 1$ and $|x|_j = 1$ for $2m+1 \leq j \leq (d+1)m$. We can therefore reproduce the determinant computation done in Section 2 replacing ε by η and U_{Stark} by the subgroup U_0 of U_K generated by U_{K+} and the conjugates of η . We get

$$(U_K : U_0) = \pm 2^{dm-1} \frac{R_{K+}}{R_K} \prod_{\chi \text{ odd}} \frac{1}{2} \sum_{g \in G} \chi(g) \log |\eta^g|.$$

We then proceed as in Theorem 2.3 by looking at the kernel of the norm map acting on $U_0/\{\pm 1\}$. Since $\bar{\eta}$ satisfies (P1), it follows that

$$2^{dm-1} \frac{R_{K+}}{R_K} \prod_{\chi \text{ odd}} \frac{1}{2} \sum_{g \in G} \chi(g) \log |\eta^g| = \pm 2^{dm-1+ts} |\text{Cl}_K^-|.$$

Then, by (2.4), we get the result

$$\prod_{\chi \text{ odd}} \frac{1}{2} \sum_{g \in G} \chi(g) \log |\eta^g| = \pm 2^{ts} \frac{h_K R_K}{h_{K+} R_{K+}} = \pm \prod_{\chi \text{ odd}} L'_{K/k,S}(0, \chi). \quad \square$$

We now turn to the study of the structure of the $\mathbb{Q}[G]$ -module $U_K^- \otimes \mathbb{Q}$. Since U_K^- is killed by $1 + \tau$, it is a $\mathbb{Q}[G]^-$ -module where $\mathbb{Q}[G]^- := e^- \mathbb{Q}[G]$ and $e^- := \frac{1}{2}(1 - \tau)$ is the sum of the idempotents of odd characters of G .⁸ Since U_K^- injects into $U_K^- \otimes \mathbb{Q}$, we will identify it with its image. The following result describes the structure of $U_K^- \otimes \mathbb{Q}$ as a Galois module.

Proposition 4.2. *The module $U_K^- \otimes \mathbb{Q}$ is a free $\mathbb{Q}[G]^-$ -module of rank 1.*

Proof. Let \mathcal{Y}_K be the \mathbb{Q} -vector space with basis the elements z in the set $S_\infty(K)$ of infinite places of K . The group G acts on \mathcal{Y}_K in the following way: z^g for $g \in G$ and $z \in S_\infty(K)$ is the infinite place defined by $x \mapsto z(x^g)$ for all $x \in K$. Denote by \mathcal{X}_K the subspace of elements $\sum_z a_z z \in \mathcal{Y}_K$ such that $\sum_z a_z = 0$. Then the two $\mathbb{Q}[G]$ -modules \mathcal{X}_K and $U_K \otimes \mathbb{Q}$ are isomorphic by a result of Herbrand and Artin [2]. Fix a $\mathbb{Q}[G]$ -isomorphism $f : U_K \otimes \mathbb{Q} \rightarrow \mathcal{X}_K$. A direct computation shows that $\mathcal{X}_K^- := f(U_K^- \otimes \mathbb{Q})$ is spanned by the vectors $\{w^\rho - w^{\rho\tau}\}_{\rho \in R}$ where w is the fixed place of K above v . In

⁸Note that $\mathbb{Q}[G]^-$ is a ring with identity e^- .

particular, \mathcal{X}_K^- is generated as a $\mathbb{Q}[G]^-$ -module by the vector $w - w^\tau$. This proves the result. \square

Corollary 4.3. *There exist $\bar{\theta} \in \bar{U}_K^-$ and $q \in \mathbb{Q}^\times$ such that*

$$\prod_{\chi \text{ odd}} \frac{1}{2} \sum_{g \in G} \chi(g) \log |\theta^g| = q \prod_{\chi \text{ odd}} L'_{K/k,S}(0, \chi).$$

Proof. From the proposition, there exists $u \in U_K^- \otimes \mathbb{Q}$ such that $U_K^- \otimes \mathbb{Q} = \mathbb{Q}[G]^- \cdot u$. We let $\bar{\theta} := n \cdot u$ where $n \in \mathbb{N}$ is large enough so that $\bar{\theta} \in U_K^-$. Then we set

$$q := \frac{(U_K^- : \mathbb{Z}[G] \cdot \bar{\theta})}{2^{e+t} |\text{Cl}_K^-|}.$$

The result follows by the proof of Proposition 4.1 *mutatis mutandis* and replacing q by $-q$ if necessary. \square

Thanks to Proposition 4.2, it is enough to study the structure of $\mathbb{Q}[G]^-$ to understand that of $U_K^- \otimes \mathbb{Q}$. Let X be the set of irreducible \mathbb{Z} -characters of G . Each $\xi \in X$ is the sum of the irreducible characters in a conjugacy class C_ξ of \hat{G} under the action of $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. For $\xi \in X$, we let $e_\xi := \sum_{\chi \in C_\xi} e_\chi \in \mathbb{Q}[G]$ be the corresponding rational idempotent where e_χ denotes the idempotent associated to the character χ . We have

$$\mathbb{Q}[G] = \bigoplus_{\xi \in X} e_\xi \mathbb{Q}[G] \simeq \bigoplus_{\xi \in X} \mathbb{Q}(\xi)$$

where $\mathbb{Q}(\xi)$ is the cyclotomic field generated by the values of any character in C_ξ . Let X_{odd} be the set of \mathbb{Z} -characters $\xi \in X$ such that one, and thus all, characters in C_ξ are odd. We have $e^- = \sum_{\xi \in X_{\text{odd}}} e_\xi$ and from the above decomposition, we get

$$\mathbb{Q}[G]^- = \bigoplus_{\xi \in X_{\text{odd}}} e_\xi \mathbb{Q}[G] \simeq \bigoplus_{\xi \in X_{\text{odd}}} \mathbb{Q}(\xi). \quad (4.6)$$

We now define $\mathbb{Z}[G]^- := e^- \mathbb{Z}[G]$ and let \mathcal{O}_G^- be the maximal order of $\mathbb{Q}[G]^-$. We have

$$\mathcal{O}_G^- = \bigoplus_{\xi \in X_{\text{odd}}} e_\xi \mathbb{Z}[G] \simeq \bigoplus_{\xi \in X_{\text{odd}}} \mathbb{Z}[\xi]. \quad (4.7)$$

Now let p be a prime number. By (4.6), we get

$$\mathbb{Q}_p[G]^- \simeq \bigoplus_{\xi \in X_{\text{odd}}} \mathbb{Q}(\xi) \otimes_{\mathbb{Q}} \mathbb{Q}_p \simeq \bigoplus_{\xi \in X_{\text{odd}}} \bigoplus_{\mathfrak{p} \in S_{\xi,p}} \mathbb{Q}(\xi)_{\mathfrak{p}} \quad (4.8)$$

where $S_{\xi,p}$ is the set of prime ideals of $\mathbb{Q}(\xi)$ above p and $\mathbb{Q}(\xi)_{\mathfrak{p}}$ is the completion of $\mathbb{Q}(\xi)$ at the prime ideal \mathfrak{p} . On the other hand, each rational character $\xi \in X$ is the sum of irreducible \mathbb{Z}_p -characters, say $\xi = \sum_{\psi \in C_{\xi,p}} \psi$, and we have

$$\mathbb{Q}_p[G]^- = \bigoplus_{\xi \in X_{\text{odd}}} \bigoplus_{\psi \in C_{\xi,p}} e_\psi \mathbb{Q}_p[G]^-.$$

Therefore there is a bijection between the prime ideals in $S_{\xi,p}$ and the characters in $C_{\xi,p}$. For \mathfrak{p} a prime ideal in $S_{\xi,p}$, we denote by $\psi_{\xi,\mathfrak{p}}$ the corresponding irreducible \mathbb{Z}_p -character. Before stating the first result, we need one more notation. Let T be a set of primes. We say that an element $u \in \mathbb{Q}[G]$ is a T -unit if $u \in \mathbb{Z}_p[G]^{-,\times}$ for all $p \notin T$ where $\mathbb{Z}_p[G]^{-,\times}$ is the group of units of $\mathbb{Z}_p[G]^-$.

Proposition 4.4. *Let M be a sub- $\mathbb{Z}[G]^-$ -module of $\mathbb{Q}[G]^-$ of finite index. Let x be an element of M such that $x\mathbb{Z}[G]^-$ has finite index inside M . Assume that y is another element of M such that*

$$(M : x\mathbb{Z}[G]^-) = (M : y\mathbb{Z}[G]^-) \quad \text{and} \quad (M^\psi : (x\mathbb{Z}_p[G]^-)^\psi) = (M^\psi : (y\mathbb{Z}_p[G]^-)^\psi)$$

for all $p \nmid |G|$ and all $\psi \in \hat{G}_p$ with ψ odd. Then there exists a unique B -unit $u \in \mathbb{Q}[G]^-$ such that $y = ux$ where B is the set of primes dividing both $|G|$ and $(M : x\mathbb{Z}[G]^-)$.

Proof. Since $\mathbb{Q}[G]^- = x\mathbb{Q}[G]^-$, there exists $u \in \mathbb{Q}[G]^-$ such that $y = ux$. Assume $y = vx$ for another $v \in \mathbb{Q}[G]^-$. Then, for all $\xi \in X_{\text{odd}}$, we have $\xi(u)\xi(x) = \xi(v)\xi(x)$. Since $\xi(x) \neq 0$, it follows that $\xi(u) = \xi(v)$ and thus by (4.6), we get $u = v$ which proves that u is unique.

Let p be a prime. Assume first that p does not divide $|G|$. Let $\xi \in X_{\text{odd}}$ and $\mathfrak{p} \in S_{\xi,p}$. Write $\psi := \psi_{\xi,\mathfrak{p}}$ and denote by $\mathbb{Z}[\xi]_{\mathfrak{p}} := \psi(\mathbb{Z}_p[G]^-)$ the ring of integers of $\mathbb{Q}(\xi)_{\mathfrak{p}}$. Then M^ψ is an ideal of $\mathbb{Z}[\xi]_{\mathfrak{p}}$ and we have

$$\frac{(M^\psi : (x\mathbb{Z}_p[G]^-)^\psi)}{(M^\psi : (y\mathbb{Z}_p[G]^-)^\psi)} = \frac{(M^\psi : \psi(y)\mathbb{Z}[\xi]_{\mathfrak{p}})}{(M^\psi : \psi(x)\mathbb{Z}[\xi]_{\mathfrak{p}})} = |\psi(u)|_{\mathfrak{p}}.$$

Thus $\psi_{\xi,\mathfrak{p}}(u)$ is a unit in $\mathbb{Z}[\xi]_{\mathfrak{p}}$ for all $\xi \in X_{\text{odd}}$ and $\mathfrak{p} \in S_{\xi,p}$ and thus u lies in $\mathbb{Z}_p[G]^{-,\times}$. Assume now that p does not divide the index $(M : x\mathbb{Z}[G]^-)$. We have

$$(M \otimes \mathbb{Z}_p : x\mathbb{Z}_p[G]^-) = (M \otimes \mathbb{Z}_p : y\mathbb{Z}_p[G]^-) = 1.$$

Therefore $x\mathbb{Z}_p[G]^- = M \otimes \mathbb{Z}_p = y\mathbb{Z}_p[G]^-$ and $u \in \mathbb{Z}_p[G]^{-,\times}$. \square

By Propositions 4.2 and 4.4, we get the following result.

Corollary 4.5. *Let B be the set of primes that divide both $|G|$ and $|\text{Cl}_K^-|$. Assume there exist $\bar{\eta}$ and $\bar{\eta}'$ two elements of U_K^- satisfying (P1) and (P2). Then there exists a unique B -unit $u \in \mathbb{Q}[G]^-$ such that $\bar{\eta}' = u \cdot \bar{\eta}$. \square*

From this result and the discussion at the beginning of the section, one cannot expect the properties (P1) and (P2) to characterize the Stark unit if $\mathbb{Z}[G]^-$ has some non trivial B -units and a fortiori if $\mathbb{Z}[G]^-$ has some non trivial units.⁹ It follows from the methods of [6] that $\mathbb{Z}[G]^-$ has some non trivial units if and only if $\mathcal{O}_{\bar{G}}$ does. By (4.7), this is the case if and only if there exists an odd character of G whose order divides 6. In particular, for G a cyclic group, $\mathbb{Z}[G]^-$ has only trivial units if and only if the order of G is at most 6. We will prove in the next sections that there exist solutions to (P1) and (P2) in these cases (with some additional conditions for sextic extensions). From this we will deduce another proof of the conjecture for quadratic extensions and a weak version of the conjecture for quartic and sextic extensions.

5. ALGEBRAIC TOOLS

In this section we introduce some algebraic tools and results that will be useful in the next sections. We start with the properties of Fitting ideals. Let R be a commutative ring with an identity element. Let M be a finitely generated R -module. Therefore there exists a surjective homomorphism $f : R^a \rightarrow M$ for some $a \geq 1$. The Fitting ideal of M as an R -module, denoted $\text{Fitt}_R(M)$, is the ideal of R generated by $\det(\vec{v}_1, \dots, \vec{v}_a)$ where $\vec{v}_1, \dots, \vec{v}_a$ run through the elements of the kernel of f . One can prove that it does not depend on the choice of f . We will use the following properties of Fitting ideals, see [8, Chap. 3] or [4, Chap. 20].

⁹If $\bar{\eta}$ is a solution to (P1) and (P2) and u is a B -unit then $u \cdot \bar{\eta}$ is not necessarily a solution to (P1) and (P2). A necessary and sufficient condition for that is that the linear map $x \mapsto ux$ of $\mathbb{Q}[G]^-$ has determinant ± 1 . This is always true if u is a unit of $\mathbb{Z}[G]^-$.

- If there exist ideals A_1, \dots, A_t of R such that

$$M \simeq R/A_1 \oplus \dots \oplus R/A_t,$$

then we have

$$\text{Fitt}_R(M) = A_1 \cdots A_t.$$

- Let T be an R -algebra. We have

$$\text{Fitt}_T(M \otimes_R T) = \text{Fitt}_R(M)T.$$

- Let N be another finitely generated R -module. We have

$$\text{Fitt}_R(M \oplus N) = \text{Fitt}_R(M)\text{Fitt}_R(N).$$

Lemma 5.1. *Let M be a finite \mathcal{O}_G^- -module. Then*

$$|M| = |(\mathcal{O}_G^- / \text{Fitt}_{\mathcal{O}_G^-}(M))|.$$

Proof. We have

$$(\mathcal{O}_G^- : \text{Fitt}_{\mathcal{O}_G^-}(M)) = \prod_{\xi \in X_{\text{odd}}} (e_\xi \mathbb{Z}[G] : e_\xi \text{Fitt}_{\mathcal{O}_G^-}(M)) = \prod_{\xi \in X_{\text{odd}}} (\mathbb{Z}[\xi] : \text{Fitt}_{\mathbb{Z}[\xi]}(e_\xi M)).$$

Fix $\xi \in X_{\text{odd}}$. Since $e_\xi M$ is a finite $\mathbb{Z}[\xi]$ -module, there exist ideals $\mathfrak{a}_1, \dots, \mathfrak{a}_r$ such that

$$e_\xi M = \mathbb{Z}[\xi]/\mathfrak{a}_1 \oplus \dots \oplus \mathbb{Z}[\xi]/\mathfrak{a}_r.$$

Therefore $\text{Fitt}_{\mathbb{Z}[\xi]}(e_\xi M) = \mathfrak{a}_1 \cdots \mathfrak{a}_r$ and

$$(\mathbb{Z}[\xi] : \text{Fitt}_{\mathbb{Z}[\xi]}(e_\xi M)) = N_{\mathbb{Q}(\xi)/\mathbb{Q}}(\mathfrak{a}_1 \cdots \mathfrak{a}_r) = |e_\xi M|.$$

It follows that $(\mathcal{O}_G^- : \text{Fitt}_{\mathcal{O}_G^-}(M)) = \prod_{\xi \in X_{\text{odd}}} |e_\xi M| = |M|$. \square

Lemma 5.2. *Let M be a finite $\mathbb{Z}[G]^-$ -module. Let p be a prime number not dividing $|G|$ and let ψ be an odd irreducible \mathbb{Z}_p -character. Then*

$$|M^\psi| = |(\mathbb{Z}[G]^- / \text{Fitt}_{\mathbb{Z}[G]^-}(M))^\psi| = |(\mathcal{O}_G^- / \text{Fitt}_{\mathcal{O}_G^-}(M))^\psi|.$$

Proof. We have $(\text{Fitt}_{\mathbb{Z}[G]^-}(M))^\psi = \text{Fitt}_{\mathbb{Z}_p[\psi]}(M^\psi)$. Since M^ψ is a finite $\mathbb{Z}_p[\psi]$ -module, there exist integers $c_1, \dots, c_r \geq 1$ such that

$$M^\psi \simeq \bigoplus_{i=1}^r \mathbb{Z}_p[\psi]/\mathfrak{p}^{c_i}$$

where \mathfrak{p} is the prime ideal of $\mathbb{Z}_p[\psi]$. Then $\text{Fitt}_{\mathbb{Z}[G]^-}(M)^\psi = \mathfrak{p}^c$ with $c := c_1 + \dots + c_r$ and therefore $|(\mathbb{Z}[G]^- / \text{Fitt}_{\mathbb{Z}[G]^-}(M))^\psi| = (\mathbb{Z}_p[\psi] : \mathfrak{p}^c) = |M^\psi|$. The last equality is clear since $(\mathcal{O}_G^-)^\psi = \mathbb{Z}_p[\psi]$. \square

In what follows we will also use repeatedly the Tate cohomology of finite cyclic groups, see [7, §IX.1]. Let A be a finite cyclic group with generator a and let M be a $\mathbb{Z}[A]$ -module. The zero-th and first group of cohomology are defined by

$$\hat{H}^0(A, M) := M^A / N_A(M) \quad \text{and} \quad \hat{H}^1(A, M) := \text{Ker}(N_A : M \rightarrow M) / (1 - a)M$$

where $N_A := \sum_{b \in A} b$ and M^A is the submodule of elements in M fixed by A . Let N and P be two other $\mathbb{Z}[A]$ -modules such that the following short sequence is exact:

$$1 \longrightarrow M \longrightarrow N \longrightarrow P \longrightarrow 1.$$

Then the hexagon below is also exact.

$$\begin{array}{ccccc}
 & & \hat{H}^0(A, M) & & \\
 & \nearrow & & \searrow & \\
 \hat{H}^1(A, P) & & & & \hat{H}^0(A, N) \\
 \uparrow & & & & \downarrow \\
 \hat{H}^1(A, N) & & & & \hat{H}^0(A, P) \\
 & \nwarrow & & \swarrow & \\
 & & \hat{H}^1(A, M) & &
 \end{array} \tag{5.9}$$

The Herbrand quotient of M is defined by

$$Q(A, M) := \frac{|\hat{H}^0(A, M)|}{|\hat{H}^1(A, M)|}.$$

The Herbrand quotient is multiplicative, that is for an exact short sequence as above, we have $Q(A, N) = Q(A, M) Q(A, P)$. The following result plays a crucial rôle in the next sections. It is a direct consequence of [7, Cor. IX.4.2].

Lemma 5.3. *Let E/F be a quadratic extension with Galois group T . Let $R \geq 0$ be the number of real places in F that becomes complex in E . Then we have*

$$Q(T, U_E) = 2^{R-1}. \quad \square$$

We use this result in the following way. Assume that $R \geq 1$. Write \bar{U}_F and \bar{U}_E for the group of units of F and E respectively modulo $\{\pm 1\}$. Then we have

$$\hat{H}^0(T, U_E) = \frac{U_F}{\mathcal{N}_{E/F}(U_E)} = \{\pm 1\} \times \frac{\bar{U}_F}{\mathcal{N}_{E/F}(\bar{U}_E)}$$

since -1 cannot be a norm in E/F . It follows from the lemma that $|\hat{H}^0(T, U_E)|$ is divisible by 2^{R-1} and therefore

$$2^{R-2} \mid (\bar{U}_F : \mathcal{N}_{E/F}(\bar{U}_F)). \tag{5.10}$$

In some cases we will not be able to get non trivial lower bounds with that method, but still be able to deduce that $\hat{H}^1(T, U_E)$ is trivial. In this situation, we have the following lemma.

Lemma 5.4. *Let E/F be a quadratic extension with Galois group T . Assume that $\hat{H}^1(T, U_E)$ is trivial. Then either E/F is unramified at finite places or there exists an element of order 2 in the kernel of the norm map from Cl_E to Cl_F .*

Proof. Consider the submodules of elements fixed by T in the short exact sequence

$$1 \longrightarrow U_E \longrightarrow E^\times \longrightarrow P_E \longrightarrow 1.$$

We get

$$1 \longrightarrow U_F \longrightarrow F^\times \longrightarrow P_E^T \longrightarrow \hat{H}^1(T, U_E) \longrightarrow \dots$$

Since $\hat{H}^1(T, U_E) = 1$ by hypothesis, it follows that the groups P_F and P_E^T are isomorphic. The isomorphism is the natural map that sends $\mathfrak{a} \in P_F$ to $\mathfrak{a}\mathbb{Z}_E \in P_E^T$, where \mathbb{Z}_E is the ring of integers of E . Assume that there is a prime ideal \mathfrak{p} of F that ramifies in E/F . Let \mathfrak{P} be the unique prime ideal of E above \mathfrak{p} and let $h \geq 1$ be the order of \mathfrak{P} in Cl_E . Since $\mathfrak{P}^h \in P_E^T$, there exists a principal ideal $\mathfrak{a} \in P_F$ such that $\mathfrak{P}^h = \mathfrak{a}\mathbb{Z}_E$. Clearly \mathfrak{a} is

a power of \mathfrak{p} . Looking at valuations at \mathfrak{P} , it follows that h is even. We set $\mathfrak{C} := \mathfrak{P}^{h/2}$. Its class is an element of order 2 in Cl_E . But $\mathcal{N}_{E/F}(\mathfrak{C}) = \mathfrak{p}^{h/2} = \mathfrak{a}$ is a principal ideal. This concludes the proof. \square

To conclude this section we prove the conjecture in our settings when K/k is a quadratic extension. This result is proved in full generality in [15, Th. IV.5.4].

Theorem 5.5. *Let K/k be a quadratic extension and $S \supset S(K/k)$ be a finite set of places of k satisfying (A1), (A2) and (A3). Then the abelian rank one Stark conjecture is satisfied for the extension K/k and the set S with the Stark unit being the unique solution, up to trivial units, of (P1) and (P2). Moreover the Stark unit is a square in K if and only if $e + t_S + c \geq 1$ where c is the 2-valuation of the order of Cl_K^- . In particular, if $d \geq 4$ then it always a square and, in fact, it is a 2^{d-3} -th power. It is also a square if $d = 3$ and the extension K/k is ramified at some finite prime.*

Proof. The only non trivial element of G is τ . Let χ be the character that sends τ to -1 . It is the only non trivial character of G and also the only odd character. We have $\mathbb{Z}[G]^- = \mathcal{O}_G^- = e^- \mathbb{Z} \simeq \mathbb{Z}$. In particular, using Proposition 4.2, it is direct to see that there exists $\bar{\theta} \in U_K^-$ such that $U_K^- = \mathbb{Z} \cdot \bar{\theta}$. Define

$$\bar{\eta} := 2^{e+t_S} |\text{Cl}_K^-| \cdot \bar{\theta}.$$

From its construction, it is clear that $\bar{\eta}$ satisfies (P1) and (P2). It follows from Proposition 4.1, and replacing η by η^{-1} if necessary, that

$$\frac{1}{2} \sum_{g \in G} \chi(g) \log |\eta^g| = L'_{K/k}(0, \chi).$$

This proves part (1) of the conjecture. Part (3) is direct by construction. It remains to prove part (2). But $(\tau - 1) \cdot \bar{\eta} = -2 \cdot \bar{\eta}$ so part (2) follows and the conjecture is proved in this case. Finally, from its definition, it is clear that η is a 2^r -th power in K^\times if and only if $e + t_S + c \geq r$. Now, by (5.10), we have $e \geq d - 3$ and therefore the Stark unit is always a square if $d \geq 4$. Assume that $d = 3$ and that η is not a square. Then $e = 0$ and $|\hat{H}^0(G, U_K)| = 2$. From Lemma 5.3, we get $\hat{H}^1(G, U_K) = 1$ and therefore, since $c = 0$, the extension K/k is unramified at finite places by Lemma 5.4 \square

When $d = 2$, there exist extensions for which the Stark unit is a square and extensions for which it is not a square. Using the PARI/GP system [16], we find the following examples.¹⁰ Let $k := \mathbb{Q}(\sqrt{5})$ and let v_1, v_2 denote the two infinite places of k with $v_1(\sqrt{5}) < 0$ and $v_2(\sqrt{5}) > 0$. Let K be the ray class field modulo $\mathfrak{p}_{11}v_2$ where $\mathfrak{p}_{11} := (1/2 + 3\sqrt{5}/2)$ is one of the two prime ideals above 11. Then K/k is a quadratic extension that satisfies (A1), (A2) and (A3) with $S := S(K/k)$, and one can prove that the corresponding Stark unit is not a square. Now, on the other hand, let K be the ray class field modulo $\sqrt{5}\mathfrak{q}_{11}v_1$, where $\mathfrak{q}_{11} := (1/2 - 3\sqrt{5}/2)$ is the other prime ideal above 11. Then K/k is a quadratic extension that satisfies (A1), (A2) and (A3) with $S := S(K/k)$ and, in this case, the Stark unit is a square. When $d = 3$ and K/k is unramified both cases are possible. Indeed, let $k := \mathbb{Q}(\alpha)$ where $\alpha^3 - \alpha^2 - 13\alpha + 1 = 0$. It is a totally real cubic field. Let v_1, v_2, v_3 be the three infinite places of k with $v_1(\alpha) \approx -3.1829$, $v_2(\alpha) \approx 0.0765$ and $v_3(\alpha) \approx 4.1064$. Let K be the ray class field of k of conductor $\mathbb{Z}_k v_2 v_3$. Then K/k is a quadratic extension that satisfies (A1), (A2) and (A3) with $S := S(K/k)$, and that is unramified at finite places. One can prove in this setting that the Stark unit is not a square. On the other hand, let $k := \mathbb{Q}(\beta)$ with $\beta^3 - \beta^2 - 24\beta - 35 = 0$. It is a totally real cubic field. Let v_1, v_2, v_3 be the three infinite places of k with $v_1(\alpha) \approx -3.0999$,

¹⁰PARI/GP was also used to find the examples given in the next two sections.

$v_2(\alpha) \approx -1.8861$, and $v_3(\alpha) \approx 5.9860$. Let K be the unique quadratic extension k of conductor $\mathbb{Z}_k v_2 v_3$. Then K/k satisfies (A1), (A2) and (A3) with $S := S(K/k)$ and is unramified at finite places. One can prove that k is principal and the class number of K is 2. Therefore the Stark unit in this case is a square.

6. CYCLIC QUARTIC EXTENSIONS

The goal of this section is to prove the following result.

Theorem 6.1. *Let K/k be a cyclic quartic extension and $S \supset S(K/k)$ be a finite set of places of k satisfying (A1), (A2) and (A3). Then there exists $\bar{\eta} \in U_K^-$ satisfying (P1) and (P2). Furthermore, $\bar{\eta}$ is unique up to the action of $\pm G$, satisfies for all $\chi \in \hat{G}$*

$$\left| L'_{K/k,S}(0, \chi) \right| = \frac{1}{2} \left| \sum_{g \in G} \chi(g) \log |\eta^g| \right|$$

and the extension $K(\sqrt{\bar{\eta}})/k$ is abelian.

Proof. Denote by γ a generator of G , therefore $\tau = \gamma^2$. Let χ be the character of G such that $\chi(\gamma) = i$ and let $\xi := \chi + \chi^3$ be the only element in X_{odd} . From the results of Section 4, we have

$$\mathbb{Q}[G]^- = e^- \mathbb{Q}[G] \simeq \mathbb{Q}(i)$$

where the ring isomorphism sends any element of $x \in \mathbb{Q}[G]^-$, written uniquely as $x = e^-(a + b\gamma)$ for $a, b \in \mathbb{Q}$, to $\chi(x) = a + bi$. In particular, we have $\mathbb{Z}[G]^- = \mathcal{O}_G^- \simeq \mathbb{Z}[i]$ and $\mathbb{Z}[G]^-$ is a principal ring. By Proposition 4.2, this implies that there exists $\bar{\theta} \in U_K^-$ such that $U_K^- = \mathbb{Z}[G]^- \cdot \bar{\theta}$.

We now prove the unicity of the solution. Assume that $\bar{\eta}$ and $\bar{\eta}'$ are two solutions to (P1) and (P2). By Corollary 4.5, there exists a unique 2-unit u in $\mathbb{Q}[G]^-$ such that $\bar{\eta}' = u \cdot \bar{\eta}$. Let $\mathfrak{p}_2 := (i + 1)\mathbb{Z}[i]$ be the unique prime ideal above 2 in $\mathbb{Z}[i]$. Let $n := v_{\mathfrak{p}_2}(\chi(u))$. Assume, without loss of generality, that $n \geq 0$ (otherwise, exchange $\bar{\eta}$ and $\bar{\eta}'$ and replace u by u^{-1}) and therefore $\bar{\eta}' \in \mathbb{Z}[G]^- \cdot \bar{\eta}$. Let $x \in \mathbb{Z}[G]^-$ be such that $\bar{\eta} = x \cdot \bar{\theta}$. We have

$$\begin{aligned} (\mathbb{Z}[G]^- \cdot \bar{\eta} : \mathbb{Z}[G]^- \cdot \bar{\eta}') &= (x\mathbb{Z}[G]^- : ux\mathbb{Z}[G]^-) \\ &= (\chi(x)\mathbb{Z}[i] : \chi(u)\chi(x)\mathbb{Z}[i]) \\ &= |\chi(u)| = 2^n. \end{aligned}$$

Therefore $n = 0$ and u is a unit. Since the only units of $\mathbb{Z}[i]$ are ± 1 and $\pm i$, it follows that $u = \pm e^-g$ with $g \in G$. This proves the unicity statement.

Next we prove that there exist solutions to (P1) and (P2). Let $\mathcal{F} := \text{Fitt}_{\mathbb{Z}[G]^-}(\text{Cl}_K^-)$ be the Fitting ideal of Cl_K^- as a $\mathbb{Z}[G]^-$ -module. Let f be a generator of \mathcal{F} . We set $\bar{\eta} := f(\gamma + 1)^{e+ts} \cdot \bar{\theta}$. We have by Lemma 5.1

$$(U_K^- : \mathbb{Z}[G] \cdot \bar{\eta}) = 2^{e+ts}(\mathbb{Z}[G]^- : \mathcal{F}) = 2^{e+ts}|\text{Cl}_K^-|.$$

Thus $\bar{\eta}$ is a solution to (P1). In the same way it follows directly from Lemma 5.2 that it is a solution to (P2).

Now, since $\bar{\eta} \in U_K^-$, we have for $\nu = \chi_0$, the trivial character, or $\nu = \chi^2$ that

$$\frac{1}{2} \sum_{g \in G} \nu(g) \log |\eta^g| = 0.$$

On the other hand, $L'_{K/k,S}(\nu, 0) = 0$ follows directly from [15, Prop. I.3.4]. From Proposition 4.1, using the fact that $\chi^3 = \bar{\chi}$, we get¹¹

$$\begin{aligned} \left| L'_{K/k,S}(0, \chi) \right|^2 &= L'_{K/k,S}(0, \chi) L'_{K/k,S}(0, \chi^3) \\ &= \left(\frac{1}{2} \sum_{g \in G} \chi(g) \log |\eta^g| \right) \left(\frac{1}{2} \sum_{g \in G} \chi^3(g) \log |\eta^g| \right) \\ &= \left| \frac{1}{2} \sum_{g \in G} \chi(g) \log |\eta^g| \right|^2 \end{aligned}$$

and the equality to be proved follows by taking square-roots.

Finally, to prove that $K(\sqrt{\eta})/k$ is abelian, we need to prove that $(\gamma - 1) \cdot \bar{\eta} \in 2 \cdot U_K^-$ by [15, Prop. IV.1.2]. This is equivalent to proving that

$$(i - 1)(i + 1)^{e+t_S} \chi(f) \in 2\mathbb{Z}[i],$$

that is one of the following assertions is satisfied: $e \geq 1$, $t_S \geq 1$ or 2 divides $|\text{Cl}_K^-|$. We have $e \geq 2d - 4$ by (5.10) and therefore the result is proved if $d \geq 3$. Assume that $d = 2$ and $e = 0$. Then it follows by Lemma 5.3 that $\hat{H}^1(T, U_K) = 1$ where $T := \langle \tau \rangle$. By Lemma 5.4 this implies that either 2 divides $|\text{Cl}_K^-|$ and the result is proved, or K/K^+ is unramified at finite places. Assume the latter. At least one prime ideal of k ramifies in K by the proof of [10, Lem. 2.8] since k is a quadratic field. By (A3) this prime ideal is inert in K/K^+ , thus $t_S \geq 1$. This concludes the proof. \square

A consequence of this result is that we can say quite precisely when the Stark unit, if it exists, is a square in that case. The result is very similar to the situation in the quadratic case (see Theorem 5.5).

Corollary 6.2. *Under the hypothesis of the theorem and assuming that the Stark unit exists, then it is a square in K if and only if $e + t_S + c \geq 2$ where c is the 2-valuation of $|\text{Cl}_K^-|$. In particular, if $d \geq 3$ then it is always a square and, in fact, it is a 2^{d-2} -th power.*

Proof. We prove the equivalence. The inequality is satisfied when the Stark unit ε is a square by Corollary 2.4. Now assume that the inequality is satisfied. By the unicity statement of the theorem, we have $\bar{\varepsilon} = \bar{\eta}$ (replacing η by one of its conjugate if necessary). From the proof of the theorem, we see that $\bar{\eta}$ belongs to $2^r \cdot U_K^-$ if and only if $(i + 1)^{e+t_S} \chi(f) \in 2^r \mathbb{Z}[i]$. Taking valuation at \mathfrak{p}_2 , the only prime ideal above 2, we see that it is equivalent to $e + t_S + c \geq 2r$. This proves the first assertion. Now, to prove the second assertion, we see that $e \geq 2d - 4$ by (5.10). Therefore $\bar{\eta}$ lies in $2^{d-2} \cdot U_K^-$. This proves the result. \square

When $d = 2$ it is possible to find examples for which the Stark unit, if it exists, is a square and examples for which it is not a square. For example, let $k := \mathbb{Q}(\sqrt{5})$ and let v_1, v_2 denote the two infinite places of k with $v_1(\sqrt{5}) < 0$ and $v_2(\sqrt{5}) > 0$. Let K be the ray class field modulo $\mathfrak{p}_{29}v_1$ where $\mathfrak{p}_{29} := (11/2 - \sqrt{5}/2)$ is one of the two prime ideals above 29. Then K/k is a cyclic quartic extension that satisfies (A1), (A2) and (A3) with $S := S(K/k)$ and one can prove that, if it exists, the Stark unit is not a square. Now, on the other hand, let K be the ray class field modulo $\sqrt{5}\mathfrak{p}_{41}v_1$ where $\mathfrak{p}_{41} := (13/2 - \sqrt{5}/2)$ is one of the two prime ideals above 41. Then K/k is a cyclic quartic extension that

¹¹Note that it is easy to see that both sides of (4.5) are positive in this case.

satisfies (A1), (A2) and (A3) with $S := S(K/k)$, but one can prove that, in this case, the Stark unit, if it exists, is a square.

7. CYCLIC SEXTIC EXTENSIONS

In this final section we study the case when K/k is a cyclic sextic extension. We will need some additional assumptions to be able to prove that there exists solutions to (P1) and (P2).

Theorem 7.1. *Let K/k be a cyclic sextic extension such that (A1), (A2) and (A3) are satisfied with $S := S(K/k)$. Assume also that 3 does not divide the order of Cl_K and that no prime ideal above 3 is wildly ramified in K/k . Let F be the quadratic extension of k contained in K . Then there exists $\bar{\eta} \in U_K^-$ satisfying (P1) and (P2) and such that $\mathcal{N}_{K/F}(\eta)$ is the Stark unit for the extension F/k and the set of places S . Furthermore, $\bar{\eta}$ is unique up to the action of an element of $\text{Gal}(K/F)$, satisfies for all $\chi \in \hat{G}$*

$$\left| L'_{K/k,S}(0, \chi) \right| = \frac{1}{2} \left| \sum_{g \in G} \chi(g) \log |\eta^g| \right|,$$

and the extension $K(\sqrt{\eta})/k$ is abelian.

Proof. Let γ be a generator of the Galois group G , thus $\tau = \gamma^3$. Let χ be the character that sends γ to $-\omega$ where ω is a fixed primitive third root of unity. It is a generator of the group of characters of G . We have $X_{\text{odd}} = \{\xi_2, \xi_6\}$ where $\xi_2 := \chi^3$ and $\xi_6 := \chi + \chi^5$. The corresponding idempotents are

$$e_{\xi_2} = \frac{1}{6}(1 - \gamma^3)(1 + \gamma^2 + \gamma^4) \quad \text{and} \quad e_{\xi_6} = \frac{1}{6}(1 - \gamma^3)(2 - \gamma^2 - \gamma^4).$$

We have the ring isomorphism

$$\mathbb{Q}[G]^- = e_{\xi_2} \mathbb{Q}[G] + e_{\xi_6} \mathbb{Q}[G] \cong \mathbb{Q} \oplus \mathbb{Q}(\omega). \quad (7.11)$$

Let $\sigma := \gamma^2$ and let H be the subgroup of order 3 generated by σ . Any element $g \in \mathbb{Q}[G]^-$ can be written uniquely as $g = e^- h$ where h is an element of $\mathbb{Q}[H]$. The map $g \mapsto h$ is a ring isomorphism between $\mathbb{Q}[G]^-$ and $\mathbb{Q}[H]$, that restricts to an isomorphism between $\mathbb{Z}[G]^-$ and $\mathbb{Z}[H]$. From now on, we will identify $\mathbb{Q}[G]^-$ and $\mathbb{Q}[H]$. Note that, with that identification, both act in the same way on $U_K^-, U_K^- \otimes \mathbb{Q}, \text{Cl}_K^-,$ etc. Let e_0 and e_1 be the image by the projection map of e_{ξ_2} and e_{ξ_6} . Then $e_0 = \frac{1}{3}(1 + \sigma + \sigma^2)$ is the idempotent of the trivial character of H and $e_1 = \frac{1}{3}(2 - \sigma - \sigma^2)$ is the sum of the idempotents of the two non trivial characters of H . The main difference between this case and the quartic case is the fact that the isomorphism between $\mathbb{Q}[H]$ and $\mathbb{Q} \oplus \mathbb{Q}(\omega)$ does not restrict to an isomorphism between $\mathbb{Z}[G]^-$ and $\mathbb{Z} \oplus \mathbb{Z}[\omega]$. In particular, $\mathbb{Z}[G]^-$ is not a principal ring. Because of that the proof is somewhat more intricate than in the quartic case. We will therefore proceed by proving a series of different claims. First, we define

$$\mathcal{O} := e_0 \mathbb{Z}[H] + e_1 \mathbb{Z}[H] \simeq \mathbb{Z} \oplus \mathbb{Z}[\omega]. \quad (7.12)$$

Note that, by the above identification, we have $\mathcal{O}_{\bar{G}} \cong \mathcal{O}$.

Claim 1. The ring \mathcal{O} is principal and contains $\mathbb{Z}[H]$ with index 3.

Let \mathcal{I} be an ideal of \mathcal{O} . Then $e_0 \mathcal{I}$ is an ideal of $e_0 \mathbb{Z} \simeq \mathbb{Z}$. Thus there exists $a \in \mathbb{Z}$ such that $e_0 \mathcal{I} = a e_0 \mathbb{Z}[H]$. In the same way, $e_1 \mathcal{I}$ is an ideal of $e_1 \mathbb{Z} \simeq \mathbb{Z}[\omega]$. Since $\mathbb{Z}[\omega]$ is a principal ring, there exists $b, c \in \mathbb{Z}$ such that $e_1 \mathcal{I} = e_1(b + c\sigma) \mathbb{Z}[H]$. One verify readily that $e_0 a + e_1(b + c\sigma)$ is a generator of \mathcal{I} . To conclude the proof of Claim 1, we note that $\mathcal{O}/\mathbb{Z}[H] = \langle e_0 + \mathbb{Z}[H] \rangle = \langle e_1 + \mathbb{Z}[H] \rangle$ clearly has order 3.

Claim 2. Let \mathcal{A} be an ideal of $\mathbb{Z}[H]$ of finite index. Then there exists $g \in \mathcal{A}$ such that

$$\mathcal{O}/\mathcal{AO} \simeq \mathbb{Z}[H]/g\mathbb{Z}[H]. \quad (7.13)$$

Furthermore, $\mathcal{A} = g\mathbb{Z}[H]$ if \mathcal{A} is a principal ideal. Otherwise $(\mathcal{A} : g\mathbb{Z}[H]) = 3$.

We prove this claim by considering the two cases: $\mathcal{AO} \neq \mathcal{A}$ and $\mathcal{AO} = \mathcal{A}$.

Claim 2.1. Assume that $\mathcal{AO} \neq \mathcal{A}$. Then \mathcal{A} is a principal ideal.

Let $g' = e_0a + e_1(b + c\sigma)$ be a generator of the principal ideal \mathcal{AO} of \mathcal{O} . If $e_1(b + c\sigma) \in \mathcal{A}$, then $e_1\mathcal{A} = e_1(b + c\sigma)\mathbb{Z}[H] \subset \mathcal{A}$ and it follows that $\mathcal{A} = \mathcal{AO}$, a contradiction. Therefore $\mathcal{AO}/\mathcal{A} = \langle e_1(b + c\sigma) + \mathcal{A} \rangle$ has order 3. Thus one of the three elements: $e_0a + e_1(b + c\sigma)$, $e_0a - e_1(b + c\sigma)$ or e_0a belongs to \mathcal{A} . It cannot be e_0a since that would imply, as above, that $\mathcal{A} = \mathcal{AO}$. Denote by g the one element between $e_0a \pm e_1(b + c\sigma)$ that lies in \mathcal{A} . Clearly we still have $g\mathcal{O} = \mathcal{AO}$. Now, g is not a zero divisor since \mathcal{A} has finite index in $\mathbb{Z}[H]$, so we have $(g\mathcal{O} : g\mathbb{Z}[H]) = (\mathcal{O} : \mathbb{Z}[H]) = 3$. Therefore we get

$$(\mathcal{A} : g\mathbb{Z}[H]) = \frac{(g\mathcal{O} : g\mathbb{Z}[H])}{(\mathcal{AO} : \mathcal{A})} = 1$$

and $\mathcal{A} = g\mathbb{Z}[H]$. Equation (7.13) follows in that case from the equality

$$(\mathcal{O} : \mathcal{AO})(\mathcal{AO} : \mathcal{A}) = (\mathcal{O} : \mathbb{Z}[H])(\mathbb{Z}[H] : \mathcal{A}) \quad (7.14)$$

and the fact that $(\mathcal{AO} : \mathcal{A}) = (\mathcal{O} : \mathbb{Z}[H])$ by the above.

Claim 2.2. Assume that $\mathcal{AO} = \mathcal{A}$. Then \mathcal{A} is not a principal ideal, but there exists $g \in \mathcal{A}$ such that $(\mathcal{A} : g\mathbb{Z}[H]) = 3$.

Let g be a generator of the principal ideal \mathcal{AO} of \mathcal{O} . Since $\mathcal{AO} = \mathcal{A}$, g lies in \mathcal{A} and we compute as above

$$(\mathcal{A} : g\mathbb{Z}[H]) = (\mathcal{AO} : g\mathcal{O})(g\mathcal{O} : g\mathbb{Z}[H]) = 3.$$

Since $(\mathcal{O} : \mathbb{Z}[H])(\mathbb{Z}[H] : \mathcal{A}) = 3(\mathbb{Z}[H] : \mathcal{A}) = (\mathcal{A} : g\mathbb{Z}[H])(\mathbb{Z}[H] : \mathcal{A}) = (\mathbb{Z}[H] : g\mathbb{Z}[H])$ and $(\mathcal{AO} : \mathcal{A}) = 1$, Equation (7.13) follows from (7.14). It remains to prove that \mathcal{A} cannot be principal in that case. In order to prove this, we need another result. Let $x \in \mathcal{O}$. By the isomorphism in (7.12), it corresponds to a pair (x_0, x_1) in $\mathbb{Z} \oplus \mathbb{Z}[\omega]$. We define the norm of x as the following quantity

$$\text{Norm}(x) := |x_0| N_{\mathbb{Q}(\omega)/\mathbb{Q}}(x_1).$$

Note that we recover the usual definition of the norm of $\mathbb{Q}[H]$ as a \mathbb{Q} -algebra. The proof of the following claim is straightforward and is left to the reader.

Claim 3. Let $x \in \mathcal{O}$ with $\text{Norm}(x) \neq 0$. Then $(\mathcal{O} : x\mathcal{O}) = \text{Norm}(x)$. If furthermore $x \in \mathbb{Z}[H]$ then $(\mathbb{Z}[H] : x\mathbb{Z}[H]) = \text{Norm}(x)$.

We now finish the proof of Claim 2.2. Assume that \mathcal{A} is principal, say $\mathcal{A} = h\mathbb{Z}[H]$. Then there exists $z \in \mathbb{Z}[H]$ such that $g = hz$ and we have $(\mathcal{O} : z\mathcal{O}) = 3$. Thanks to the above claim, we can explicitly compute all the elements $z \in \mathcal{O}$ such that $(\mathcal{O} : z\mathcal{O}) = 3$. There are the elements $z = e_0a + e_1(b + c\sigma)$ with $a = \pm 1$ and $b + c\sigma \in \{\pm(1 + 2\sigma), \pm(2 + \sigma), \pm(1 - \sigma)\}$, or $a = \pm 3$ and $b + c\sigma \in \{\pm 1, \pm\sigma, \pm(1 + \sigma)\}$. One can compute all possibilities and check that none of those belong to $\mathbb{Z}[H]$. This gives a contradiction and concludes the proof of Claim 2.2 and of Claim 2.

We now turn to the $\mathbb{Z}[H]$ -structure of U_K^- . The principal result is the following claim that we will prove in several steps.

Claim 4. There exists $\bar{\theta} \in U_K^-$ such that $U_K^- = \mathbb{Z}[H] \cdot \bar{\theta}$.

Let $\bar{\theta}' \in U_K^-$ be such that $U_K^- \otimes \mathbb{Q} = \mathbb{Q}[H] \cdot \bar{\theta}'$. Note that the existence of $\bar{\theta}'$ follows from Proposition 4.2. We define

$$\Lambda := \{x \in \mathbb{Q}[H] : x \cdot \bar{\theta}' \in U_K^-\}.$$

It is a fractional ideal of $\mathbb{Z}[H]$. The above claim is satisfied if and only if it is a principal ideal. Assume that this is not the case. Then, by the above, we have¹² $\Lambda\mathcal{O} = \Lambda$. Recall that F denotes the subfield of K fixed by H . It is a quadratic extension of k and $\text{Gal}(F/k) = \langle \tau \rangle$. We define U_F^- as the kernel of the norm map from $U_F/\langle \pm 1 \rangle$ to $U_k/\langle \pm 1 \rangle$. We have also $U_F^- = U_K^- \cap (F^\times / \langle \pm 1 \rangle)$. Let $N_H := 1 + \sigma + \sigma^2$. It is the group ring element corresponding to the norm of the extensions K/F and K^+/k .

Claim 4.1. $\Lambda\mathcal{O} = \Lambda$ if and only if $N_H \cdot U_K^- = 3 \cdot U_F^-$. If $\Lambda\mathcal{O} \neq \Lambda$, then $N_H \cdot U_K^- = U_F^-$.

We have $\Lambda\mathcal{O} = \Lambda$ if and only if $e_0\Lambda \subset \Lambda$, that is $N_H \cdot U_K^- \subset 3 \cdot U_K^-$. Assume that it is the case. Let $\bar{\delta} \in U_K^-$ and set $\kappa := N_{K/F}(\bar{\delta}) \in U_F$. Then the polynomial $X^3 - \kappa$ has a root, say ν , in U_K . If ν does not belong to F then all the roots of $X^3 - \kappa$ belongs to K since K/F is a Galois extension. It follows that K contains the third roots of unity, a contradiction. Therefore $\bar{\nu} \in U_F^-$ and $N_H \cdot U_K^- \subset 3 \cdot U_F^-$. The other inclusion is trivial and the first assertion of the claim is proved. If $\Lambda\mathcal{O} \neq \Lambda$ then $3 \cdot U_F^- \subsetneq N_H \cdot U_K^- \subset U_F^-$. Since U_F^- is a \mathbb{Z} -module of rank 1, it follows that $N_H \cdot U_K^- = U_F^-$. The claim is proved.

Let \mathcal{S} be the set of prime ideals of K that are totally split in K/k . Denote by $I_{K,\mathcal{S}}$ the subgroup of I_K , the group of ideals of K , generated by the prime ideals in \mathcal{S} . Then, by Chebotarev's theorem, the following short sequence is exact

$$1 \longrightarrow P_K \cap I_{K,\mathcal{S}}^{1-\tau} \longrightarrow I_{K,\mathcal{S}}^{1-\tau} \longrightarrow \text{Cl}_K^{1-\tau} \longrightarrow 1$$

where P_K is the group of principal ideals of K . We take the Tate cohomology of this sequence for the action of H . Since 3 does not divide the order of Cl_K , it does not divide the order of $\text{Cl}_K^{1-\tau}$ and $\hat{H}^0(\text{Cl}_K^{1-\tau}) = \hat{H}^1(\text{Cl}_K^{1-\tau}) = 1$. Note that here and in what follows, to simplify the presentation, we drop the group H in the notation of the cohomology groups and write $\hat{H}^i(M)$ instead of $\hat{H}^i(H, M)$ for M a $\mathbb{Z}[H]$ -module. It follows from the exact hexagon (5.9) for the above exact sequence that $\hat{H}^i(P_K \cap I_{K,\mathcal{S}}^{1-\tau}) \simeq \hat{H}^i(I_{K,\mathcal{S}}^{1-\tau})$ for $i = 0, 1$. Let $\mathfrak{A} \in P_K \cap I_{K,\mathcal{S}}^{1-\tau}$. There exist $\alpha \in K_S^\times$, the subgroup of elements of K^\times supported only by prime ideals in \mathcal{S} , and $\mathfrak{B} \in I_{K,\mathcal{S}}$ such that

$$\mathfrak{A} = (\alpha) = \mathfrak{B}^{1-\tau}.$$

We apply $1 - \tau$ to this equation

$$\mathfrak{A}^{1-\tau} = (\alpha)^{1-\tau} = \mathfrak{B}^{(1-\tau)^2} = (\mathfrak{B}^{1-\tau})^2 = \mathfrak{A}^2.$$

Therefore we have $(P_K \cap I_{K,\mathcal{S}}^{1-\tau})^2 \subset P_{K,\mathcal{S}}^{1-\tau}$ where $P_{K,\mathcal{S}}$ is the subgroup of principal ideals generated by the elements of K_S^\times . It follows that the quotient $(P_K \cap I_{K,\mathcal{S}}^{1-\tau})/P_{K,\mathcal{S}}^{1-\tau}$ is killed by 2 and therefore $\hat{H}^i(P_K \cap I_{K,\mathcal{S}}^{1-\tau}) = \hat{H}^i(P_{K,\mathcal{S}}^{1-\tau})$ for $i = 0$ or 1 . We have proved the following claim.

Claim 4.2. $\hat{H}^0(P_{K,\mathcal{S}}^{1-\tau}) \simeq \hat{H}^0(I_{K,\mathcal{S}}^{1-\tau})$ and $\hat{H}^1(P_{K,\mathcal{S}}^{1-\tau}) \simeq \hat{H}^1(I_{K,\mathcal{S}}^{1-\tau})$.

Let $u \in U_K \cap (K_S^\times)^{1-\tau}$. There exists $\alpha \in K_S^\times$ such that $u = \alpha^{1-\tau}$. Therefore we get

$$u^{1-\tau} = \alpha^{(1-\tau)^2} = (\alpha^{1-\tau})^2 = u^2.$$

¹²Strictly speaking, the claims above are only for integral ideals of $\mathbb{Z}[H]$ but they admit obvious and direct generalizations to fractional ideals.

Reasoning as above, this implies that $\hat{H}^i(U_K \cap (K_S^\times)^{1-\tau}) = \hat{H}^i(U_K^{1-\tau}) = \hat{H}^i(U_K^-)$ for $i = 0, 1$. We now consider the short exact sequence

$$1 \longrightarrow U_K \cap (K_S^\times)^{1-\tau} \longrightarrow (K_S^\times)^{1-\tau} \longrightarrow P_{K,S}^{1-\tau} \longrightarrow 1.$$

Taking the Tate cohomology and using the above equalities, we extract the following exact sequence from the exact hexagon (5.9) corresponding to this exact sequence

$$\cdots \longrightarrow \hat{H}^1(P_{K,S}^{1-\tau}) \longrightarrow \hat{H}^0(U_K^-) \longrightarrow \hat{H}^0((K_S^\times)^{1-\tau}) \longrightarrow \cdots \quad (7.15)$$

The next claim is just a reformulation of the first part of Claim 4.1.

Claim 4.3. $\Lambda\mathcal{O} = \Lambda$ if and only if $\hat{H}^0(U_K^-) \simeq \mathbb{Z}/3\mathbb{Z}$.

Assume the two followings claims for the moment.

Claim 4.4. $\hat{H}^1(P_{K,S}^{1-\tau})$ is trivial.

Claim 4.5. $\hat{H}^0((K_S^\times)^{1-\tau})$ is trivial.

By (7.15) we get that $\hat{H}^0(U_K^-) = 1$. Thus $\Lambda\mathcal{O} \neq \mathcal{O}$ by Claim 4.3 and therefore Λ is principal by Claim 2.1, and Claim 4 follows. It remains to prove Claims 4.4 and 4.5. We start with the proof of Claim 4.4. By Claim 4.2, this is equivalent to prove that $\hat{H}^1(I_{K,S}^{1-\tau})$ is trivial. We have as $\mathbb{Z}[H]$ -modules

$$I_{K,S}^{1-\tau} = \prod'_{\mathfrak{p}_0 \in \mathcal{S}_0} \left(\prod_{\mathfrak{P}|\mathfrak{p}_0} \mathfrak{P}^{\mathbb{Z}} \right)^{1-\tau} \simeq \prod'_{\mathfrak{p}_0 \in \mathcal{S}_0} (1-\tau)\mathbb{Z}[G]$$

where \mathcal{S}_0 is the set of prime ideals of k that splits completely in K/k , \mathfrak{P} runs through a set of representative of the prime ideals of K dividing \mathfrak{p}_0 under the action of τ and the $'$ indicates that it is a restricted product, that is the exponent of \mathfrak{P} is zero for all but finitely many prime ideals. The isomorphism comes from fixing a prime ideal above \mathfrak{p}_0 and the fact that \mathfrak{p}_0 is totally split in K/k . Therefore we have

$$\hat{H}^1(I_{K,S}^{1-\tau}) = \prod'_{\mathfrak{p}_0 \in \mathcal{S}_0} \hat{H}^1((1-\tau)\mathbb{Z}[G]) \simeq \prod'_{\mathfrak{p}_0 \in \mathcal{S}_0} \hat{H}^1(\mathbb{Z}[H]).$$

It is well-known that $\hat{H}^1(\mathbb{Z}[H]) = 1$, thus Claim 4.4 is proved.

To prove Claim 4.5, we prove that the norm from $(K_S^\times)^{1-\tau}$ to $(F_S^\times)^{1-\tau}$ is surjective. Let $\alpha^{1-\tau} \in (F_S^\times)^{1-\tau}$. By the Hasse Norm Principle, $\alpha^{1-\tau}$ is a norm in K/F if and only if it is a norm in $K_{\mathfrak{P}}/F_{\mathfrak{p}}$ for all prime ideals \mathfrak{P} of K where \mathfrak{p} denotes the prime ideal of F below \mathfrak{P} . If \mathfrak{p} splits in K/F , then $\alpha^{1-\tau}$ is trivially a norm in $K_{\mathfrak{P}}/F_{\mathfrak{p}}$. Assume now that \mathfrak{p} is inert. It follows from the theory of local fields, see [7, §XI.4], that the norm of $K_{\mathfrak{P}}/F_{\mathfrak{p}}$ is surjective on the group of units of $F_{\mathfrak{p}}$. But $\alpha^{1-\tau}$ is a unit at \mathfrak{P} since $\mathfrak{P} \notin \mathcal{S}$, and therefore it is a norm also in this case. Finally we assume that \mathfrak{P} is ramified in K/F . Let p be the rational prime below \mathfrak{P} . By hypothesis, $p \neq 3$ since 3 is not wildly ramified in K/k . Write $\mu_{\mathfrak{P}}$, $\mathbb{U}_{\mathfrak{P}}$, $\mu_{\mathfrak{p}}$ and $\mathbb{U}_{\mathfrak{p}}$ for the group of roots of unity of order prime to p and the group of principal units of $K_{\mathfrak{P}}$ and $F_{\mathfrak{p}}$ respectively. We have $\mu_{\mathfrak{P}} = \mu_{\mathfrak{p}}$ and therefore $\mathcal{N}_{K_{\mathfrak{P}}/F_{\mathfrak{p}}}(\mu_{\mathfrak{P}}) = \mu_{\mathfrak{p}}^3$. On the other hand $\mathcal{N}_{K_{\mathfrak{P}}/F_{\mathfrak{p}}}(\mathbb{U}_{\mathfrak{P}}) = \mathbb{U}_{\mathfrak{p}}^3 = \mathbb{U}_{\mathfrak{p}}$ and the norm is surjective on principal units. Since $\mathfrak{P} \notin \mathcal{S}$, $v_{\mathfrak{P}}(\alpha) = 0$ and $\alpha = \zeta u$ with $\zeta \in \mu_{\mathfrak{p}}$ and $u \in \mathbb{U}_{\mathfrak{p}}$. It follows from the above discussion that $\alpha^{1-\tau}$ is a norm in $K_{\mathfrak{P}}/F_{\mathfrak{p}}$ if and only if $\zeta^{1-\tau} \in \mu_{\mathfrak{p}}^3$. Let \mathfrak{p}_0 be the prime ideal of k below \mathfrak{p} . Assume first that \mathfrak{p}_0 is ramified in F/k . Then $\mu_{\mathfrak{p}} \subset k_{\mathfrak{p}_0}$ and $\zeta^{1-\tau} = 1$, thus $\alpha^{1-\tau}$ is a norm in $K_{\mathfrak{P}}/F_{\mathfrak{p}}$. Assume now that \mathfrak{p}_0 is inert¹³ in F/k . Denote by f the residual degree of \mathfrak{p}_0 . The group

¹³By (A3), it cannot be split in F/k .

$\mu_{\mathfrak{p}_0}$ of roots of unity in $k_{\mathfrak{p}_0}$ of order prime to p has order $p^f - 1$. Let $\mathfrak{P}^+ := \mathfrak{P} \cap K^+$. The extension $K_{\mathfrak{P}^+}^+/k_{\mathfrak{p}_0}$ is a tamely ramified cyclic cubic extension. Therefore it is a Kummer extension by [7, Prop. II.5.12] and $k_{\mathfrak{p}_0}$ contains the third roots of unity, that is 3 divides $p^f - 1$. Since τ is the Frobenius element at \mathfrak{p}_0 of the extension F/k , we have $\zeta^{1-\tau} = \zeta^{1-p^f} = (\zeta^{(1-p^f)/3})^3 \in \mu_{\mathfrak{p}}^3$ and therefore $\alpha^{1-\tau}$ is a norm in $K_{\mathfrak{P}}/F_{\mathfrak{p}}$. We have proved that $\alpha^{1-\tau}$ is a norm everywhere locally. It follows by the Hasse Norm Principle that there exists $\beta \in K^\times$ such that $\mathcal{N}_{K/F}(\beta) = \alpha^{1-\tau}$. Let \mathfrak{P} be a prime ideal of K not in \mathcal{S} and, as above, let \mathfrak{p} be the prime ideal of F below \mathfrak{P} . Assume first that \mathfrak{P} is ramified or inert in K/F , then $v_{\mathfrak{P}}(\beta) = v_{\mathfrak{p}}(\alpha^{1-\tau})$ or $\frac{1}{3}v_{\mathfrak{p}}(\alpha^{1-\tau})$ respectively. In both cases we get $v_{\mathfrak{P}}(\beta) = 0$ since $\alpha \in K_{\mathcal{S}}^\times$. If \mathfrak{P} is split in K/F then it must be inert or ramified in K/K^+ by (A3). It follows that $v_{\mathfrak{P}}(\beta^{1-\tau}) = 0$. Therefore $\delta := \beta^{1-\tau} \in K_{\mathcal{S}}^\times$. We now compute

$$\mathcal{N}_{K/F}(\delta^{1-\tau}) = \mathcal{N}_{K/F}(\beta)^{(1-\tau)^2} = (\alpha^{1-\tau})^{2(1-\tau)} = (\alpha^{1-\tau})^4.$$

Thus $\alpha^{1-\tau}$ is the norm of $(\delta/\alpha)^{1-\tau} \in (K_{\mathcal{S}}^\times)^{1-\tau}$. This concludes the proof of Claim 4.5 and therefore also the proof of Claim 4. The next claim follows from Claim 4.1 and the fact, seen in the proof of Claim 4, that $\Lambda\mathcal{O} \neq \Lambda$.

Claim 5. $N_H \cdot U_K^- = U_F^-$.

Let $\mathcal{F} := \text{Fitt}_{\mathbb{Z}[H]}(\text{Cl}_K^-)$ be the Fitting ideal of Cl_K^- as a $\mathbb{Z}[H]$ -module. Apply Claim 2 to the ideal \mathcal{F} and call f the element of \mathcal{F} such that $\mathcal{O}/\mathcal{F}\mathcal{O} \simeq \mathbb{Z}[H]/f\mathbb{Z}[H]$. Set $\bar{\eta}' := f \cdot \bar{\theta}$. Thanks to Claim 4, we find that

$$(U_K^- : \mathbb{Z}[H] \cdot \bar{\eta}') = (\mathbb{Z}[H] : f\mathbb{Z}[H]) = (\mathcal{O} : \mathcal{F}\mathcal{O}) = |\text{Cl}_K^-|. \quad (7.16)$$

For this last equality, we first use the fact that, since 3 does not divide the order of Cl_K^- , we can make e_0 and e_1 act on it and see it therefore as an \mathcal{O} -module. By the properties of the Fitting ideal, $\mathcal{F}\mathcal{O}$ is the Fitting ideal of Cl_K^- as an \mathcal{O} -module and the equality follows from Lemma 5.1.

Claim 6. Let $n, m \geq 0$ be two integers. Then there exists $\kappa_{n,m} \in \mathbb{Z}[H]$, unique up to a trivial unit, such that

$$\text{Norm}(\kappa_{n,m}) = 2^{n+2m} \quad \text{and} \quad e_0 \kappa_{n,m} = e_0 2^n. \quad (7.17)$$

We define

$$\kappa_{n,m} := 2^n e_0 + (-1)^{n+m} 2^m e_1.$$

It is clear from its construction that $\kappa_{n,m}$ satisfies (7.17). One can see also directly that $\kappa_{n,m} \in \mathbb{Z}[H]$ since $2 \equiv -1 \pmod{3}$. It remains to prove the unicity statement. Clearly $e_0 \kappa_{n,m}$ is fixed by construction. On the other hand $e_1 \kappa_{n,m}$ is an element of norm 2^{2m} in $e_1 \mathbb{Z}[H] \simeq \mathbb{Z}[\omega]$. Since 2 is inert in $\mathbb{Z}[\omega]$, there exists only one element in $\mathbb{Z}[\omega]$ of norm 2^{2m} up to units. This concludes the proof of the claim.

Let $e' \in \mathbb{N}$ be such that $2^{e'} = (\bar{U}_k : \mathcal{N}(\bar{U}_F))$. We now prove the following claim.

Claim 7. The integer $e - e'$ is non-negative and even.

We consider the natural map $\bar{U}_k \rightarrow \bar{U}_{K^+}/\mathcal{N}(\bar{U}_K)$ that comes from the inclusion $U_k \subset U_{K^+}$. Let $\bar{u} \in \bar{U}_k$ be in the kernel of this map. Thus there exists $\bar{x} \in \bar{U}_K$ such that $\bar{u} = \mathcal{N}(\bar{x})$. Set $\bar{y} := N_H \cdot \bar{x} - \bar{u} \in \bar{U}_F$. We have

$$\mathcal{N}(\bar{y}) = N_H \cdot \mathcal{N}(\bar{x}) - \mathcal{N}(\bar{u}) = 3 \cdot \bar{u} - 2 \cdot \bar{u} = \bar{u}.$$

Therefore the kernel of the above map is $\mathcal{N}(\bar{U}_F)$ and there is a well-defined injective group homomorphism from $\bar{U}_k/\mathcal{N}(\bar{U}_F)$ to $\bar{U}_{K+}/\mathcal{N}(\bar{U}_K)$. This proves that¹⁴ $e \geq e'$. The cokernel of this map is

$$\frac{\bar{U}_{K+}/\mathcal{N}(\bar{U}_K)}{\bar{U}_k/\mathcal{N}(\bar{U}_F)} \simeq \bar{U}_{K+}/(\bar{U}_k + \mathcal{N}(\bar{U}_K)). \quad (7.18)$$

It is a finite $\mathbb{Z}[H]$ -module of order $2^{e-e'}$. In particular, the idempotents e_0 and e_1 act on it. We have $e_0 \cdot \bar{U}_{K+}/(\bar{U}_k + \mathcal{N}(\bar{U}_K)) = N_H \cdot \bar{U}_{K+}/(\bar{U}_k + \mathcal{N}(\bar{U}_F)) = 1$. It follows that $\bar{U}_{K+}/(\bar{U}_k + \mathcal{N}(\bar{U}_K)) = e_1 \cdot \bar{U}_{K+}/(\bar{U}_k + \mathcal{N}(\bar{U}_K))$ is a $\mathbb{Z}[\omega]$ -module. Since 2 is inert in $\mathbb{Z}[\omega]$, the order of $\bar{U}_{K+}/(\bar{U}_k + \mathcal{N}(\bar{U}_K))$ is an even power of 2. This concludes the proof of the claim.

Let $\kappa := \kappa_{e'+t_S, (e-e')/2}$. We define

$$\bar{\eta} := \pm \kappa \cdot \bar{\eta}'. \quad (7.19)$$

The choice of the sign will be done during the proof of the next claim. We have

$$\begin{aligned} (U_K^- : \mathbb{Z}[H] \cdot \bar{\eta}) &= (U_K^- : \mathbb{Z}[H] \cdot \bar{\eta}')(\mathbb{Z}[H] \cdot \bar{\eta}' : \mathbb{Z}[H]\kappa \cdot \bar{\eta}') \\ &= |\text{Cl}_K^-| \text{Norm}(\kappa) = 2^{e+t_S} |\text{Cl}_K^-| \end{aligned}$$

using (7.16), Claim 3 and the definition and properties of κ . Therefore, $\bar{\eta}$ satisfies (P1). Let p be a prime not dividing $[K : k]$ and let ψ be an odd irreducible \mathbb{Z}_p -character. By the construction of $\bar{\eta}'$, the fact that p is odd and κ is a 2-unit, we find that

$$|(U_K^-/\mathbb{Z}[H] \cdot \bar{\eta})^\psi| = |(U_K^-/\mathbb{Z}[H] \cdot \bar{\eta}')^\psi| = |(\mathcal{O}/\mathcal{F})^\psi| = |(\text{Cl}_K^-)^\psi|.$$

The last equality comes from Lemma 5.2. This proves that $\bar{\eta}$ is also a solution to (P2).

The next step is to prove the following result.

Claim 8. Up to the right choice of sign in (7.19), we have

$$\frac{1}{2} \sum_{g \in G} \chi^3(g) \log |\eta^g|_w = L'_{K/k, S}(0, \chi^3).$$

The $\mathbb{Z}[H]$ -module $U_K^-/(\mathbb{Z}[H] \cdot \bar{\eta})$ has order not divisible by 3 since $\bar{\eta}$ satisfies (P1). Thus it is a \mathcal{O} -module and we can split it into two parts corresponding to the two idempotents e_0 and e_1 . On one side, using Claim 5, we have

$$e_0 \cdot (U_K^-/\mathbb{Z}[H] \cdot \bar{\eta}) = N_H \cdot (U_K^-/\mathbb{Z}[H] \cdot \bar{\eta}) \simeq U_F^-/\mathbb{Z} \cdot \bar{\eta}_F$$

where $\bar{\eta}_F := N_H \cdot \bar{\eta} \in U_F^-$. On the other side, we compute

$$e_1 \cdot (U_K^-/\mathbb{Z}[H] \cdot \bar{\eta}) \simeq e_1(\mathbb{Z}[H]/\kappa f\mathbb{Z}[H]) \simeq \mathbb{Z}[\omega]/2^{(e-e')/2} \mathcal{F}_1$$

where \mathcal{F}_1 is the Fitting ideal of $(\text{Cl}_K^-)^{e_1}$ viewed as an $\mathbb{Z}[\omega]$ -module. Indeed, we have by construction

$$e_1 f\mathbb{Z}[H] = e_1 \mathcal{F}\mathcal{O} \simeq \text{Fitt}_{\mathbb{Z}[\omega]}((\text{Cl}_K^-)^{e_1}).$$

Since $\text{Cl}_K^- = (\text{Cl}_K^-)^{e_0} \oplus (\text{Cl}_K^-)^{e_1}$ and $(\text{Cl}_K^-)^{e_0} \simeq \mathcal{N}_{K/F}(\text{Cl}_K^-)$, we have

$$(\mathbb{Z}[\omega] : \mathcal{F}_1) = |(\text{Cl}_K^-)^{e_1}| = \frac{|\text{Cl}_K^-|}{|\mathcal{N}_{K/F}(\text{Cl}_K^-)|}.$$

Claim 8.1. $\mathcal{N}_{K/F}(\text{Cl}_K^-) = \text{Cl}_F^-$.

¹⁴This inequality follows also from Claim 10 below.

Consider the composition of maps $\text{Cl}_F^- \rightarrow \text{Cl}_K^- \rightarrow \text{Cl}_F^-$ where the first map is the map induced by the lifting of ideals from F to K and the second map is the norm $\mathcal{N}_{K/F}$. The map constructed in that way is the multiplication by 3 and therefore, if the order of Cl_F^- is not divisible by 3, it is a bijection and the claim is proved. Assume that 3 divides the order of Cl_F^- . Let h_E denote the class number of a number field E . Thus $h_K^- := |\text{Cl}_K^-| = h_K/h_{K^+}$ and $h_F^- := |\text{Cl}_F^-| = h_F/h_k$. If K/F is ramified at some finite prime then h_F divides h_K . As h_F^- divides h_F , it follows that $3 \mid h_K$, a contradiction. Assume now that K/F is unramified at finite primes. Therefore 3 divides h_F and $h_F/3$ divides h_K . In the same way, K^+/k is unramified and therefore 3 divides h_k . Since $3 \mid h_F^-$, this implies that 9 divides h_F and therefore 3 divides h_K , a contradiction. It follows that 3 does not divide $|\text{Cl}_F^-|$ and the claim is proved.

Putting together the claim and the computation that precedes it, we find that

$$(U_F^- : \mathbb{Z} \cdot \bar{\eta}_F) = \frac{(U_K^- : \mathbb{Z} \cdot \bar{\eta})}{2^{e-e'}} \frac{|\text{Cl}_F^-|}{|\text{Cl}_K^-|} = 2^{e'+t_S} |\text{Cl}_F^-|. \quad (7.20)$$

Let $\mathfrak{P}^+ \in S_{K^+}$ and denote by \mathfrak{p}_0 the prime ideal of k below \mathfrak{P}^+ . Then \mathfrak{P}^+ is inert in K/K^+ if and only if \mathfrak{p}_0 is inert in F/k . Furthermore, if \mathfrak{P}^+ is inert in K/K^+ , then it is ramified¹⁵ in K^+/k and it is the only prime ideal in S_{K^+} above \mathfrak{p}_0 . It follows that the number t_S of prime ideals in S_{K^+} that are inert in K/K^+ is equal to the number of prime ideals in S that are inert in F/k . Therefore $\bar{\eta}_F$ satisfy the properties (P1) and (P2) for the extension F/k and the set of primes S . As a consequence of Theorem 5.5, we see that either η_F or η_F^{-1} is the Stark unit for the extension K/F and the set of places S . By choosing the right sign in (7.19), we can assume that η_F is the Stark unit. Therefore we have

$$\frac{1}{2}(\log |\eta_F|_w + \nu(\tau) \log |\eta_F^\tau|_w) = L'_{F/k,S}(0, \nu)$$

where ν is the non trivial character of F/k . It follows from the functorial properties of L -functions that $L_{F/k,S}(s, \nu) = L_{K/k,S}(s, \chi^3)$, and from the definition of η_F that

$$\log |\eta_F|_w + \nu(\tau) \log |\eta_F^\tau|_w = \sum_{g \in G} \chi^3(g) \log |\eta^g|_w.$$

This completes the proof of the claim.

Now, by Proposition 4.1, we know that

$$\begin{aligned} \left(\frac{1}{2} \sum_{g \in G} \chi(g) \log |\eta^g| \right) \left(\frac{1}{2} \sum_{g \in G} \chi^3(g) \log |\eta^g| \right) \left(\frac{1}{2} \sum_{g \in G} \chi^5(g) \log |\eta^g| \right) \\ = \pm L'_{K/k,S}(0, \chi) L'_{K/k,S}(0, \chi^3) L'_{K/k,S}(0, \chi^5). \end{aligned}$$

We cancel the non zero terms corresponding to χ^3 using Claim 8 and, since χ and χ^5 are conjugate, we get

$$\begin{aligned} \left| \frac{1}{2} \sum_{g \in G} \chi(g) \log |\eta^g| \right|^2 &= \left(\frac{1}{2} \sum_{g \in G} \chi(g) \log |\eta^g| \right) \left(\frac{1}{2} \sum_{g \in G} \chi^5(g) \log |\eta^g| \right) \\ &= L'_{K/k,S}(0, \chi) L'_{K/k,S}(0, \chi^5) = |L'_{K/k,S}(0, \chi)|^2. \end{aligned}$$

¹⁵Recall that $S = S(K/k)$.

Taking square-roots, we get

$$\left| \frac{1}{2} \sum_{g \in G} \chi(g) \log |\eta^g| \right| = \left| \frac{1}{2} \sum_{g \in G} \chi^5(g) \log |\eta^g| \right| = |L'_{K/k,S}(0, \chi)| = |L'_{K/k,S}(0, \chi^5)|.$$

Note that we have directly using [15, Prop. I.3.4]

$$\begin{aligned} \frac{1}{2} \sum_{g \in G} \chi_0(g) \log |\eta^g| &= \frac{1}{2} \sum_{g \in G} \chi^2(g) \log |\eta^g| = \frac{1}{2} \sum_{g \in G} \chi^4(g) \log |\eta^g| \\ &= L'_{K/k,S}(0, \chi_0) = L'_{K/k,S}(0, \chi^2) = L'_{K/k,S}(0, \chi^4) = 0. \end{aligned}$$

We now prove that $\bar{\eta}$ is unique up to multiplication by an element of H . Assume that $\bar{\eta}'$ is another element of U_K^- satisfying (P1), (P2) and such that $N_H \cdot \bar{\eta}'$ is the Stark unit for the extension F/k and the set of places S . Let $u \in \mathbb{Q}[H]$ be such that $\bar{\eta}' = u \cdot \bar{\eta}$. By Corollary 4.5, u is a 2-unit. Now, by hypothesis, $\bar{\eta}_F = N_H \cdot (u \cdot \bar{\eta}) = u \cdot (N_H \cdot \bar{\eta}) = u \cdot \bar{\eta}_F$ and thus $e_0 u = e_0$. Write u_1 for the element of $\mathbb{Q}(\omega)$ such that $(1, u_1)$ corresponds to u by the isomorphism in (7.11). Since both $\bar{\eta}$ and $\bar{\eta}'$ satisfy (P1), we have $\text{Norm}(u) = 1$ and thus $N_{\mathbb{Q}(\omega)/\mathbb{Q}}(u_1) = 1$. But u_1 is a 2-unit in $\mathbb{Q}(\omega)$ and there is only prime ideal above 2 in $\mathbb{Q}(\omega)$. Therefore u_1 is in fact a unit and $u \in H$.

Finally, it remains to prove that $K(\sqrt{\eta})/k$ is an abelian extension. As noted before this is equivalent to prove that $(\gamma - 1) \cdot \bar{\eta} \in 2 \cdot \bar{U}_K^-$ by [15, Prop. IV.1.2]. Now γ acts on U_K^- as $-\sigma^2$. Thus, by the definition of $\bar{\eta}$ and the isomorphism between U_K^- and $\mathbb{Z}[H]$, this is equivalent to prove that

$$(\sigma^2 + 1)\kappa f \in 2\mathbb{Z}[H]. \quad (7.21)$$

Claim 9. Let $x \in \mathbb{Z}[H]$. Then $x \in 2\mathbb{Z}[H]$ if and only if $xe_0 \in 2e_0\mathbb{Z}[H]$ and $xe_1 \in 2e_1\mathbb{Z}[H]$.

If $x \in 2\mathbb{Z}[H]$ then clearly $xe_0 \in 2e_0\mathbb{Z}[H]$ and $xe_1 \in 2e_1\mathbb{Z}[H]$. Reciprocally, assume that $xe_0 = 2e_0a_0$ and $xe_1 = 2e_1a_1$ with $a_0, a_1 \in \mathbb{Z}[H]$. Let $a := e_0a_0 + e_1a_1$. We have by construction $2a = x \in \mathbb{Z}[H]$ and $3a = (3e_0)a_0 + (3e_1)a_1 \in \mathbb{Z}[H]$. Therefore a belongs to $\mathbb{Z}[H]$ and the claim is proved.

We prove (7.21) using the claim. On one hand, we have

$$e_0(\sigma^2 + 1)\kappa f = 2^{e' + ts + 1}e_0f \in 2e_0\mathbb{Z}[H].$$

On the other hand, we have

$$e_1(\sigma^2 + 1)\kappa f = 2^{(e - e')/2}e_1(\sigma^2 + 1)f.$$

The proof will be complete if we prove that $e - e' > 0$. For that we use the following claim.

Claim 10. $|\hat{H}^0(T, U_K/U_F)| = 2^{e - e'}$.

Let U_K° be the subgroup of elements $u \in U_K$ such that $u^{1-\tau} \in U_F$. We have

$$\begin{aligned} \hat{H}^0(T, U_K/U_F) &= \frac{(U_K/U_F)^T}{\mathcal{N}(U_K/U_F)} = \frac{U_K^\circ/U_F}{(\mathcal{N}(U_K)U_F)/U_F} \\ &\simeq \frac{U_K^\circ}{\mathcal{N}(U_K)U_F} \simeq \frac{\bar{U}_K^\circ}{\mathcal{N}(\bar{U}_K) + \bar{U}_F}. \end{aligned}$$

By (7.18), it is enough to prove the following group isomorphism

$$\bar{U}_{K^+}/(\mathcal{N}(\bar{U}_K) + \bar{U}_k) \simeq \bar{U}_K^\circ/(\mathcal{N}(\bar{U}_K) + \bar{U}_F). \quad (7.22)$$

Since $\bar{U}_{K+} \cap (\mathcal{N}(\bar{U}_K) + \bar{U}_F) = \mathcal{N}(\bar{U}_K) + \bar{U}_k$, there is a natural injection of the LHS of (7.22) in the RHS induced by the inclusion $\bar{U}_{K+} \subset \bar{U}_K^\circ$. We prove now that this map is surjective. Let $\bar{u} \in \bar{U}_K^\circ$. Thus $\bar{x} := (1 - \tau) \cdot \bar{u} \in \bar{U}_F$. Note that $(1 - \tau) \cdot \bar{x} = 2 \cdot \bar{x}$. Define $\bar{y} := N_H \cdot \bar{u} - \bar{x} \in \bar{U}_F$ and $\bar{z} := \bar{u} - \bar{y}$. We have

$$(1 - \tau) \cdot \bar{z} = (1 - \tau) \cdot \bar{u} - (1 - \tau)N_H \cdot \bar{u} + (1 - \tau) \cdot \bar{x} = \bar{x} - N_H \cdot \bar{x} + 2 \cdot \bar{x} = 0.$$

Thus $\bar{z} \in \bar{U}_{K+}$. This proves that $\bar{u} = \bar{z} + \bar{y} \in \bar{U}_{K+} + \bar{U}_F$. Equation (7.22) follows and the proof of the claim is finished.

Now by the multiplicativity of the Herbrand quotient and Lemma 5.3, we find that

$$Q(T, U_K/U_F) = \frac{Q(T, U_K)}{Q(T, U_F)} = 2^{2d-2}. \quad (7.23)$$

Therefore $e - e' \geq 2d - 2 \geq 2$. This concludes the proof that $K(\sqrt{\eta})$ is abelian over k and the proof of the theorem. \square

Corollary 7.2. *Under the hypothesis of the theorem and assuming that the Stark unit exists, then it is a square in K if and only if the Stark unit for the extension F/k and the set S is a square and $(e - e')/2 + c - c' \geq 1$ where c is the 2-valuation of $|\text{Cl}_K^-|$, c' is the 2-valuation of $|\text{Cl}_F^-|$ and $(\bar{U}_k : \mathcal{N}(\bar{U}_F)) = 2^{e'}$. In particular, if $d \geq 4$ then it is always a square and, in fact, it is a 2^{d-3} -th power. It is also a square if $d = 3$ and the extension K/k is ramified at some finite prime.*

Proof. We use the notations and results of the proof of the theorem. By the unicity statement, the Stark unit, if it exists, is equal to η or one of this conjugate over F . In particular, the Stark unit is a 2^r -th power in K if and only if $\bar{\eta} \in 2^r \cdot U_K^-$. By Claim 9 and the construction of $\bar{\eta}$, this is equivalent to

$$2^{e'+t_S} e_0 f \in 2^r e_0 \mathbb{Z} \quad \text{and} \quad 2^{(e-e')/2} e_1 f \in 2^r e_1 \mathbb{Z}[H].$$

Now $e_0 f \mathbb{Z} = e_0 |\text{Cl}_F^-| \mathbb{Z}$ by the definition of f , Claim 8.1 and the discussion that precedes it. Thus the first condition is equivalent to $e' + t_S + c' \geq r$. For $r = 1$, this is equivalent to the fact that the Stark unit for F/k and the set S is a square by Theorem 5.5 and the discussion that follows (7.20) on the number of primes in S that are inert in F/k . For the second condition, recall that $e_1 f \mathbb{Z}[H] \simeq \text{Fitt}_{\mathbb{Z}[\omega]}((\text{Cl}_K^-)^{e_1})$ and therefore $e_1 f \in 2^v \mathbb{Z}[H]$ where v is the 2-valuation of the index $(\mathbb{Z}[\omega] : \text{Fitt}_{\mathbb{Z}[\omega]}((\text{Cl}_K^-)^{e_1}))$. By Claim 8.1 and the computation before it, this index is equal to $|\text{Cl}_K^-|/|\text{Cl}_F^-|$. Therefore the second condition is equivalent to $(e - e')/2 + c - c' \geq r$. This proves the first assertion: the Stark unit for K/k and $S = S(K/k)$ is a square if and only if the Stark unit for the extension F/k and the set S is a square and $(e - e')/2 + c - c' \geq 1$. For the second assertion, we have $e' \geq d - 3$ by (5.10) and $(e - e')/2 \geq d - 1$ by Claim 10 and (7.23). Thus $\bar{\eta} \in 2^{d-3} \cdot U_K^-$ for $d \geq 4$ and we have that the Stark unit is a 2^{d-3} -th power if $d \geq 4$. Finally, for $d = 3$, the condition $2^{(e-e')/2} e_1 f \in 2e_1 \mathbb{Z}[H]$ is always satisfied. Assume that the extension K/k is ramified at some finite prime. If F/k is also ramified at some finite prime then the Stark unit for the extension F/k and the set S is a square by Theorem 5.5. If F/k is unramified at finite primes then any prime ideal that ramifies in K/k is inert in F/k by (A3). Therefore $t_S \geq 1$ and the Stark unit for the extension F/k and the set S is also a square by Theorem 5.5. It follows that the Stark unit for K/k is a square by the first part. This concludes the proof. \square

Note that the condition in the case $d = 3$ is sharp. Indeed let $k := \mathbb{Q}(\alpha)$, where $\alpha^3 + \alpha^2 - 9\alpha - 8 = 0$, be the smallest totally real cubic field of class number 3. Let v_1, v_2, v_3 be the three infinite places of k with $v_1(\alpha) \approx -3.0791$, $v_2(\alpha) \approx -0.8785$ and $v_3(\alpha) \approx 2.9576$. Let K be the ray class field of k of modulus $\mathbb{Z}_k v_2 v_3$. The extension K/k

is cyclic of order 6, satisfies (A1), (A2) and (A3) with $S := (S/k)$, and is unramified at finite places. One can check that, if it exists, the corresponding Stark unit is not a square in K .

REFERENCES

- [1] T. Arakawa. On the Stark-Shintani conjecture and certain relative class numbers. In *Automorphic forms and number theory (Sendai, 1983)*, volume 7 of *Adv. Stud. Pure Math.*, pages 1–6. North-Holland, Amsterdam, 1985.
- [2] E. Artin. Über Einheiten relativ galoisscher Zahlkörper. *J. Reine Angew. Math.*, 167:153–156, 1932.
- [3] H. Cohen and X.-F. Roblot. Computing the Hilbert class field of real quadratic fields. *Math. Comp.*, 69(231):1229–1244, 2000.
- [4] D. Eisenbud. *Commutative algebra*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995.
- [5] C. Greither and C. Popescu. An equivariant main conjecture in Iwasawa theory and applications. *J. Algebraic Geom.*, to appear, 2013.
- [6] G. Higman. The units of group-rings. *Proc. London Math. Soc. (2)*, 46:231–248, 1940.
- [7] S. Lang. *Algebraic number theory*, volume 110 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1994.
- [8] D. G. Northcott. *Finite free resolutions*. Cambridge University Press, Cambridge, 1976. Cambridge Tracts in Mathematics, No. 71.
- [9] C. Popescu. Rubin’s integral refinement of the abelian Stark conjecture. In *Stark’s conjectures: recent work and new directions*, volume 358 of *Contemp. Math.*, pages 1–35. Amer. Math. Soc., Providence, RI, 2004.
- [10] X.-F. Roblot. Stark’s conjectures and Hilbert’s twelfth problem. *Experiment. Math.*, 9(2):251–260, 2000.
- [11] K. Rubin. Stark units and Kolyvagin’s “Euler systems”. *J. Reine Angew. Math.*, 425:141–154, 1992.
- [12] H. Stark. L -functions at $s = 1$. III. Totally real fields and Hilbert’s twelfth problem. *Advances in Math.*, 22(1):64–84, 1976.
- [13] H. Stark. Hilbert’s twelfth problem and L -series. *Bull. Amer. Math. Soc.*, 83(5):1072–1074, 1977.
- [14] H. Stark. L -functions at $s = 1$. IV. First derivatives at $s = 0$. *Adv. in Math.*, 35(3):197–235, 1980.
- [15] J. Tate. *Les conjectures de Stark sur les fonctions L d’Artin en $s = 0$* , volume 47 of *Progress in Mathematics*. Birkhäuser Boston Inc., Boston, MA, 1984.
- [16] The PARI Group, Université Bordeaux 1. *PARI/GP*. Available from <http://pari.math.u-bordeaux.fr/>.
- [17] L. Washington. *Introduction to cyclotomic fields*, volume 83 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1997.

UNIVERSITÉ DE LYON, CNRS UMR 5208, UNIVERSITÉ LYON 1, INSTITUT CAMILLE JORDAN, 43
BLVD. DU 11 NOVEMBRE 1918, 69622 VILLEURBANNE CEDEX, FRANCE
E-mail address: roblot@math.univ-lyon1.fr